ПРОЛЕТАРІИ ВСѢХЪ СТРАНЪ, СОЕДИНЯЙТЕСЬ!

Всеобщій Евр. Раб. Союзъ въ Литвѣ, Польшѣ и Россіи (Бундъ).

A. BOUNDOVETZ. — L'ART DE CHIFFRER.

А. БУНДОВЕЦЪ.

ШИФРОВАННОЕ ПИСЬМО

Критика употребляемыхъ у насъ системъ шифра.

(Съ 72 таблицами и чертежами).

Изданіе Всеобщаго Еврейскаго Рабочаго Союза
въ Литвѣ, Польшѣ и Россіи.

ЖЕНЕВА.

Imprimerie israelite, Rue de Carouge 81. Geneve, Suisse

Апрѣль 1904 года.

Оглавленіе.

ПРОЛЕТАРІИ ВСѢХЪ СТРАНЪ, СОЕДИНЯЙТЕСЬ!

Всеобщій Евр. Раб. Союзъ въ Литвѣ, Польшѣ и Россіи (Бундъ).

А. БУНДОВЕЦЪ.

ШИФРОВАННОЕ ПИСЬМО

Критика употребляемыхъ у насъ системъ шифра.

Изданіе Всеобщаго Еврейскаго Рабочаго Союза въ Литвѣ, Польшѣ и Россіи.

ЖЕНЕВА.

Апрѣль 1904 года.

Предисловіе.

Предлагаемая вниманію товарищей книга посвящена по преимуществу обзору и критикѣ практикующихся у насъ системъ шифра. Продолжительный опытъ убѣдилъ насъ въ полнѣйшемъ отсутствіи среди дѣйствующихъ товарищей въ Россіи какихъ бы то ни было, хотя бы самыхъ минимальныхъ, свѣдѣній объ этомъ важномъ предметѣ. Искусству шифра никто не учитъ и не учится. Какъ во времена средневѣковья алхимическія формулы, такъ въ настоящее время тотъ или другой „рецептъ" системы передается отъ одного къ другому безъ критики и безъ пониманія. Считается какъ бы признаннымъ, что шифръ принадлежитъ къ тѣмъ секретнымъ предметамъ, о которыхъ надо говорить шепотомъ и которыхъ отнюдь не подобаетъ выносить на свѣтъ божій. Между тѣмъ—это крупная и вредная ошибка, которая на руку только Департаменту Полиціи. Нѣтъ у насъ ни одной системы, которая не была бы извѣстна спеціальному бюро шифровъ въ Петербургѣ, у котораго накопился долголѣтній громадный опытъ; мы же блуждаемъ въ потемкахъ и шифруемъ такъ, что надъ нашей простодушной наивностью въ „бюро", вѣроятно, злорадно, хохочутъ. Отъ критики нашихъ системъ мы можемъ только выиграть: неудовлетворительныя будутъ безвозвратно изгнаны и отойдутъ въ область преданій; надежныя и прочныя не боятся дневного свѣта.

Наша цѣль — дать товарищамъ вполнѣ ясное представленіе о непригодности той или другой системы. Поэтому онъ не долженъ бояться потерять понапрасну время надъ чтеніемъ кропотливаго анализа. Кто сказалъ бы, что этими анализами мы облегчаемъ лишь работу бюро, тотъ высказалъ бы тѣмъ мысль, что для бюро, состоящаго изъ спеціалистовъ, накопившаго колоссальный опытъ, могутъ показаться новыми изложенные здѣсь пріемы, опирающіеся на относительно краткій единоличный практическій опытъ.

Хотя мы старались принять во вниманіе всѣ употребляемые нашими революціонерами системы шифра, тѣмъ не менѣе, нѣкоторыя изъ нихъ могли остаться намъ неизвѣстными. Мы были бы очень обязаны товарищамъ, если бы о таковыхъ намъ сообщалось для будущихъ дополненій. Такихъ системъ, обнародованіе которыхъ неудобно, т. е. системъ, основанныхъ на какомъ-нибудь фокусѣ, мы здѣсь не приводимъ и впредь приводить не будемъ.

Авторъ.

ШИФРОВАННОЕ ПИСЬМО.

ВВЕДЕНІЕ.

I. НЕОСТОРОЖНОСТЬ и ПРЕДАТЕЛЬСТВО.

Игра нешуточна, и осторожность
Излишняя все лучше, чѣмъ небрежность.
Шиллеръ, „Пикколомини".

Почему вы такъ о немъ полагаете?... — загудѣлъ въ свою очередь Остродумовъ: — Басановъ человѣкъ съ характеромъ; онъ никого не выдастъ. А что до осторожности... знаете что? Не всякому дано быть осторожнымъ, г-нъ Паклинъ!
Тургеневъ, „Новь".

По мѣрѣ того, какъ развивается революціонное движеніе, правительство все болѣе совершенствуетъ свои средства борьбы съ нимъ.

Увеличивается штатъ Департамента Полиціи, городскихъ полицій, жандармскихъ управленій, пограничной стражи; заводятся новыя охранныя отдѣленія, вводится всюду „усиленная охрана"; „институтъ" дворниковъ преобразуется на петербургскій ладъ. Каждый успѣхъ техники оно утилизируетъ для борьбы съ крамолой: желѣзныя дороги, телеграфы, карманные фотографическіе аппараты, а въ скоромъ времени, вѣроятно, и безпроволочные телеграфы и... рентгеновскіе лучи.

Армія шпіоновъ и провокаторовъ становится колоссальной и давно уже играетъ доминирующую роль въ ловлѣ революціонеровъ. „Зубатовскіе пріемы тонкаго сыска" распространены на всю Россію. Растетъ численность шпіоновъ, изощряется ихъ опытъ и нюхъ, совершенствуются и разнообразятся ихъ пріемы. Въ настоящее время шпіонская часть такъ организована, такъ централизована, что, конечно, ни одна страна въ мірѣ никогда не создавала ничего подобнаго. Каждый изъ „агентовъ" ежедневно отправляетъ свои бюллетени въ Департаментъ Полиціи, гдѣ они сортируются, разносятся по рубрикамъ; выдѣляется часть личностей для немедленнаго обыска и ареста, часть оставляется про запасъ и для дальнѣйшаго наблюденія.

Провокаторовъ тьма. Почти нѣтъ ни одного дѣла, гдѣ бы не фигурировалъ такъ или иначе провокаторъ. Но лишь небольшая часть ихъ открывается и становится извѣстной; остальные, неразоблаченные, сохраняя свою маску, остаются въ организаціи и продолжаютъ руками жандармовъ косить революціонеровъ.

Успѣхи городской полиціи особенно замѣтны на демонстраціяхъ. Многія описанія крупныхъ демонстрацій полны, увы, болѣе восхваленіемъ „великолѣпной", „превосходной" организаціи полиціи, чѣмъ стройности и согласованности дѣйствій рабочихъ массъ. Повсюду констатируется „прогрессъ" въ дѣйствіяхъ администраціи по части подавленія, чувствуется подвижность, отсутствіе рутины. Правительство скорѣе преувеличиваетъ, чѣмъ уменьшаетъ силы революціонеровъ, и для укрѣпленія своихъ позицій не брезгаетъ ничѣмъ. Оно, съ одной стороны, пытается внести раздоръ въ ряды борющагося пролетаріата при помощи зубатовской политики натравливанія рабочихъ на интеллигентовъ, русскихъ на „инородцевъ"; съ другой стороны, оно безпрерывно и усиленно вылавливаетъ революціонеровъ, съ третьей — желаетъ навести ужасъ судебными приговорами и порками, а, съ четвертой — развратить помилованіями и подачками. Руководимое такимъ могучимъ стимуломъ, какъ само-

сохраненіе, подвижное, какъ самъ произволъ, оно быстро мѣняетъ тактику, сообразуясь съ условіями.

Если теперь отъ такой приспособляемости нашего врага, обогащающагося опытомъ и становящагося все искуснѣе, мы обратимся къ соціалдемократическимъ организаціямъ, то контрастъ выйдетъ больно ужъ рѣзкимъ. Разсматривая вопросъ исключительно съ точки зрѣнія конспиративной ловкости и выдержки нашихъ революціонеровъ, мы видимъ, что они не только стоятъ несравненно ниже дѣятелей Народной Воли, но почти не дѣлаютъ успѣховъ изъ году въ годъ. Повсюду систематическіе массовые провалы, которые далеко не свидѣтельствуютъ даже объ обиліи совершающейся работы и по поводу которыхъ никоимъ образомъ нельзя утѣшиться пословицей, что „гдѣ лѣсъ рубятъ, тамъ щепки летятъ". Часто массовые провалы съ разгромомъ организаціи бываютъ послѣ первой же прокламаціи, послѣ перваго открытаго выступленія, а въ другихъ мѣстахъ даже и до такого выступленія. Происходитъ же это въ значительной степени отъ того, что конспиративнымъ пріемамъ *учить* считается у насъ совершенно лишнимъ и непривычнымъ дѣломъ; о нихъ не говорятъ, не дебатируютъ, не пишутъ; они стоятъ на заднемъ планѣ, какъ вещь второстепенная или сама собой подразумѣвающаяся. Предполагается какъ бы, что конспиративные пріемы даются отъ рожденія или пріобрѣтаются практикой, но не изучаются,— взглядъ безусловно невѣрный и вредный. Конечно, есть люди и люди: одни — болѣе замкнутые, способные крѣпко держать тайну, другіе—болѣе откровенные и болтливые; одни—болѣе ловкіе, зоркіе, находчивые, умѣющіе легко увернуться отъ шпіоновъ, найтись въ минуту опасности, а другіе—близорукіе, ненаблюдательные, безъ развитой памяти въ отношеніи лицъ, легко теряющіеся въ трудныя минуты; есть люди проницательные, подозрительные, способные сразу раскусить провокатора, и есть люди довѣрчивые, готовые раскрыть свою душу первому встрѣчному „товарищу". Но при всѣхъ такихъ неизбѣжныхъ врожденныхъ различіяхъ, они въ значительной степени компенсируются *знаніемъ*, широкимъ и продуманнымъ знакомствомъ, какъ съ видами угрожающихъ опасностей, такъ и съ методами отъ нихъ увернуться. Если не собственный опытъ, то случаи съ товарищами, надлежащимъ образомъ проанализированные и освѣщенные, могутъ исправить присущую намъ всѣмъ халатность. Сколько людей, арестованныхъ при первомъ самостоятельномъ шагѣ, при первой попыткѣ приступить къ работѣ, съ горькой укоризной обращались къ руководителямъ, почему они не научили ихъ никакимъ пріемамъ и мѣрамъ предосторожности; сколько людей, обманутыхъ на допросахъ жандармами и наговорившихъ лишнее, плакались потомъ, что ихъ не научили даже, какъ держать себя на допросахъ.

Разсчитывать, что „практика" въ каждомъ подходящемъ человѣкѣ выработаетъ нужные пріемы и опытность—вредная ошибка. Если по такому методу дѣйствуютъ главари, то они, быть можетъ, еще и успѣютъ немного поумнѣть, потому что ихъ ошибки отражаются, до поры до времени, ближайшимъ образомъ на другихъ, а не на нихъ самихъ; но даже и въ этомъ случаѣ ошибки зачастую не освѣщаются, не обобщаются, и вслѣдствіе этого опытность пріобрѣтается однобокая. Сегодня Х. отправляетъ человѣка съ корзинкой литературы, такъ тяжело нагруженной, что она заподазривается и арестуется вмѣстѣ съ пассажиромъ; поэтому въ другой разъ онъ будетъ, быть можетъ, очень остороженъ при новыхъ посылкахъ литературы, но это не помѣшаетъ ему завтра послать письмо по ненадежному адресу, послѣ завтра захватить съ собой шпіона и т. д., и т. д. Для рядового же дѣятеля первая замѣченная имъ ошибка обыкновенно бываетъ роковой, ибо прежде совершенные промахи, остававшіеся безнаказанными, имъ не замѣчались. Сова Минервы вылетаетъ для него только ночью, въ тюрьмѣ, когда бываетъ ужъ нѣсколько поздно. Какъ мало такая одинокая, распознанная ошибка можетъ научить уму-разуму, до какой степени пріобрѣтаемая тюремная опытность остается однобокой — показываетъ быстрота, съ какой попадаются обыкновенно рецидивисты, лишь только они снова приступаютъ къ работѣ.

Всякій промахъ, хотя бы жертвой его былъ только его авторъ, вреденъ для организаціи, ибо лишаетъ ее работника. Но какъ же великъ этотъ вредъ, если результатомъ неосторожности одного является цѣлый рядъ жертвъ, бывшихъ до того совершенно неизвѣстными жандармамъ! Если Х. безъ всякой нужды хранитъ у себя важные документы, карточки, списки адресовъ, и у него ихъ отбираютъ при обыскѣ, и на основаніи добытыхъ матеріаловъ производится цѣлая облава, то такую „неосторожность" не справедливѣе ли будетъ квалифицировать, какъ преступленіе? Если У.,

приглашенный для переговоровъ въ другой городъ, привозитъ съ собой шпіона и съ этимъ хвостомъ, ни разу не оглядываясь, шествуетъ съ квартиры на квартиру, уготовляя обильную жатву для жандармовъ, то не будетъ ли это преступленіемъ? Не преступленіе ли также, если Z., встрѣтившись съ совершенно незнакомымъ человѣкомъ, о которомъ онъ судитъ лишь по его собственнымъ словамъ и по паролю, и, повѣривъ ему, что имѣетъ дѣло съ виднымъ революціонеромъ, начинаетъ ему разсказывать такія вещи, которыхъ не имѣетъ права сообщать даже самому близкому человѣку? А такіе факты бываютъ сплошь и рядомъ.

Спрашивается, велика ли разница между такими дѣяніями и поступкомъ того, кто по неопытности или легкомыслію пробалтывается на допросахъ передъ жандармами? А между тѣмъ факты послѣдняго сорта никогда не оставляются безъ разбора; они бросаютъ сильнѣйшую тѣнь на виновниковъ, которые исключаются изъ организаціи или даже объявляются предателями. Но дѣянія перваго типа никогда не обсуждаются, по нимъ не выносится приговоровъ; они признаются какъ бы естественными, неизбѣжными. Мало того, если сколько-нибудь сознательный дѣятель, будучи арестованъ, *признаетъ* только обвиненіе противъ себя, чѣмъ не повредитъ ни другимъ, ни себѣ, то это встрѣтитъ осужденіе (и совершенно справедливо), но если кто-нибудь въ той же тюрьмѣ глупо написанной и перехваченной запиской дастъ цѣнныя улики противъ сидящихъ и вызоветъ новые аресты, то такіе поступки не привлекаютъ вниманія и не вызываютъ разбирательства.

Ясно, что такой порядокъ дѣлъ ненормаленъ, страшно вреденъ. Безразличное отношеніе къ проявленіямъ безпечности и халатности родитъ новыя ихъ проявленія. Организація заинтересована въ томъ, чтобы ея силы крѣпли и развивались, чтобы ея дѣятели работали долго и успѣшно, и кто такъ или иначе приноситъ ей вредъ, долженъ быть судимъ. „Неосторожность" должна быть разсматриваема, какъ одинъ изъ видовъ „вреднаго дѣянія".

„Вредное дѣяніе", какъ въ коммерческомъ мірѣ банкротство, должно классифицироваться на три разряда: *несчастное*, *неосторожное* и *злостное*. Послѣдній разрядъ, т. е. предательство, долженъ караться самымъ безпощаднымъ образомъ; первый, гдѣ дѣло идетъ о роковыхъ случайностяхъ, конечно, ненаказуемъ. Зато средняя группа „неосторожныхъ вредныхъ дѣяній" не можетъ оставаться безъ внимательнаго разслѣдованія и вынесенія соотвѣтственнаго приговора: выговора, временнаго устраненія и полнаго удаленія изъ организаціи.

Принципы конспираціи и пріемы конспиративной техники должны какъ можно шире и глубже пропагандироваться и устно и въ печати. Неправѣ тѣ, которые думаютъ, что о нихъ неудобно писать: врядъ ли есть хоть одинъ изъ пріемовъ революціонной техники, который не былъ бы извѣстенъ жандармамъ. Тѣмъ не менѣе, нѣкоторые методы придется исключить для того, чтобы не привлечь къ нимъ усиленнаго вниманія нашихъ враговъ: за этими небольшими исключеніями, обо всемъ остальномъ можно вполнѣ свободно и говорить, и дебатировать, и писать. Какой интересный, поучительный матеріалъ представило бы, напр., печатаніе современныхъ политическихъ процессовъ по даннымъ, извѣстнымъ хотя бы только арестованнымъ: какая ближайшая причина вызвала арестъ, что найдено, какія послѣдствія для другихъ имѣли найденныя вещи, о чемъ спрашивали на допросахъ, какъ держались жандармы и заключенные, не было ли провокаторовъ, какъ дѣйствовали провокаторы, какъ они попали въ организацію, какую роль играли шпіоны, и т. д., и т. д. Въ дѣйствительности ничего подобнаго мы не имѣемъ, и вообще вопросъ о конспиративной техникѣ весьма рѣдко затрагивается, да и то въ самой общей формѣ, оставляющей мало впечатлѣнія *). Совѣты только тогда могутъ оказать вліяніе, когда они конкретизируются на частныхъ случаяхъ, на примѣрахъ, на обширной казуистикѣ.

---

*) Напр., въ № 25 „Искры" мы читаемъ слѣдующее: „Слѣдуетъ ожидать, что специфическіе пріемы зубатовскаго болѣе тонкаго сыска станутъ примѣняться болѣе систематически по всей Россіи. Въ виду этого обращаемъ вниманіе всѣхъ товарищей на необходимость ‚подтянуться' и подтянуть болѣе молодыхъ дѣятелей со стороны конспиративной постановки революціонной работы. Возможно болѣе осторожности съ адресами, выборомъ псевдонимовъ, въ устройствѣ конспиративныхъ квартиръ, въ употребленіи шифровъ. Возможно болѣе строгое отношеніе къ себѣ и къ своимъ сотрудникамъ. Возможно болѣе активное воздѣйствіе на неопытныхъ со стороны болѣе

Ближайшія причины, влекущія за собой аресты, можно классифицировать такъ:

1. *Шпіоны.* Предохранить себя отъ опасности заноса этихъ злокачественныхъ бациллъ въ здоровыя мѣста, можно только, постоянно помня объ этой возможности и тщательно слѣдя за собой на улицѣ и за своей квартирой. Для этого надо, конечно, знать всѣ пріемы шпіоновъ и способы отъ нихъ ускользать. Все это должно быть изложено въ спеціальной брошюрѣ „О шпіонахъ".

2. *Провокаторы и предатели.* Бороться съ этимъ зломъ можно посредствомъ цѣлесообразной организаціи, широкаго и глубокаго внѣдренія правилъ конспираціи и осторожнымъ, умѣлымъ выборомъ людей. Все это должно быть изложено въ брошюрахъ объ „Организаціи" и „Конспираціи".

3. *Письменные документы* (рукописи, адреса, письма простыя и шифрованныя, фотографическія карточки и пр.), какъ найденные при обыскѣ, такъ и перехваченные, или добытые другимъ путемъ. Этому вопросу, т. е. преимущественно „Шифрованному письму" посвящена настоящая брошюра.

4. *Неумѣлое поведеніе на допросахъ.* Это зло можетъ быть въ значительной степени ослаблено широкимъ распространеніемъ здравыхъ понятій о томъ, „какъ держать себя на допросахъ".

5. *Захватъ на мѣстѣ преступленія.* Къ этой категоріи мы относимъ тѣ случаи, когда революціонеры вступаютъ въ открытую борьбу, посредствомъ демонстрацій, стачекъ, собраній подъ открытымъ небомъ, террористическихъ актовъ. Аресты тутъ бываютъ часто неизбѣжны и о „неосторожности" говорить здѣсь не приходится. Однако, и въ этихъ случаяхъ громадное значеніе имѣетъ: а) знаніе пріемовъ, при помощи которыхъ можно ускользнуть изъ рукъ полиціи; б) правильная организація предпріятія, при которой уменьшается число жертвъ, напр., отбитіе арестованныхъ демонстрантовъ, защита ораторовъ на собраніяхъ отъ глазъ сыщиковъ, отказъ посылать депутатовъ для переговоровъ съ начальствомъ; в) принятіе предупредительныхъ мѣръ, чтобы захваченныя жертвы не влекли за собой новыхъ, вслѣдствіе, напримѣръ, найденныхъ у первыхъ документовъ. Все это должно быть изложено въ соотвѣтственныхъ очеркахъ.

6. *„Случайность".* Къ этой обширной и разнообразной категоріи относятся всѣ тѣ случаи, когда обнаруженіе революціонера и его арестъ производится неожиданно не только для него, но и для самихъ правительственныхъ чиновъ, когда какое-нибудь роковое случайное обстоятельство обращаетъ на него вниманіе и его изобличаетъ. Представимъ себѣ, напр. что X. везетъ съ собой въ ручномъ чемоданѣ литературу и, никѣмъ не подозрѣваемый, спокойно сидитъ въ вагонѣ. Вдругъ оказывается, что у кого-то выкрадена цѣнная вещь, начинается переполохъ и производится повальный обыскъ. Нашъ революціонеръ, благодаря совершенно постороннимъ обстоятельствамъ, попадается, какъ куръ во щи. Или положимъ, что въ домѣ, гдѣ помѣщается нелегальная типографія, происходитъ пожаръ; являются пожарные, начинаютъ ломать крышу и натыкаются на неожиданную находку. Одна типографія чуть-чуть не провалилась отъ того, что вслѣдствіе доноса акцизнаго чиновника искали по всему дому тайную винокурню.

Какъ часто говорятъ, что такого-то человѣка или такое-то предпріятіе провалила „чистая случайность". Но если вдуматься въ каждый фактъ и тщательно его проанализировать, то въ громадномъ большинствѣ случаевъ окажется, что случайность имѣетъ мѣсто только по отношенію къ полицейскимъ или жандармамъ, нашедшимъ то, чего они не искали, но никоимъ образомъ обстоятельства провала не могутъ быть названы случайными для самихъ жертвъ. Весь строй россійской жизни до такой степени пропитанъ сыскомъ, шпіонствомъ „агентовъ", полицейскихъ, дворниковъ, квартирныхъ хозяевъ, прислуги и всякихъ добровольцевъ, что добыча должна

опытныхъ, въ интересахъ революціоннаго воспитанія первыхъ". И все. Въ одномъ изъ номеровъ „Южн. Рабочаго" была недурная статейка о шпіонахъ. Въ „Искрѣ" же помѣщена была небольшая замѣтка о необходимости быть осторожнымъ при посылкѣ писемъ черезъ оказіи. Къ этой замѣткѣ намъ придется дальше вернуться. Болѣе повезло вопросу о томъ, „какъ держать себя на допросахъ": кромѣ брошюры Бахарева, носящей это названіе, были небольшія замѣтки въ нѣкоторыхъ періодическихъ органахъ (напр., „Рев. Рос.". „Искрѣ"). Въ 1897 году появилась, по сообщенію товарищей, гектографированная брошюра: „Будь мужественъ, какъ левъ, и мудръ, какъ змій". Судя по отзывамъ, она трактовала довольно поверхностно о нѣкоторыхъ вопросахъ конспираціи. Намъ она, къ сожалѣнію, не попадалась.

попадаться и тогда, когда о ней вовсе и не думаютъ въ данный моментъ; мелкая оплошность, промахъ, упущеніе революціонеровъ часто становятся для нихъ роковыми. Въ громадномъ большинствѣ случаевъ такое упущеніе можетъ быть доказано, и самый поверхностный анализъ покажетъ, что оно могло отлично и не имѣть мѣста и что провалъ никоимъ образомъ не былъ неизбѣженъ и причина его лежитъ не въ роковой „случайности", а въ простой, обыкновенной „неосторожности". Если вы спросите, напр., что провалило превосходно обставленную кишиневскую типографію, то навѣрное получите въ отвѣтъ: случайность! Одинъ изъ типографіи, будучи нелегальнымъ, былъ узнанъ шпіономъ на вокзалѣ и задержанъ—это одна случайность; въ полицейскомъ управленіи приставъ вспомнилъ, что часто видалъ его заходящимъ въ такой то дворъ—это вторая случайность. Но, спрашивается, произошелъ ли бы этотъ провалъ, если бы работавшій въ типографіи не ходилъ такъ часто по улицѣ, что обратилъ даже на себя невольно вниманіе пристава, и если бы онъ не посѣщалъ такого завѣдомо опаснаго мѣста, какъ вокзалъ? А при такихъ промахахъ не ясно ли заранѣе, что типографія не будетъ долговѣчна. Или возьмемъ провалъ типографіи въ Нѣжинѣ, которую погубила опять-таки „случайность". Фельдфебель сосѣдней казармы обратилъ вниманіе на то, что въ слесарной мастерской, недавно появившейся по близости, очень поздно виденъ свѣтъ въ окнахъ. Это показалось ему подозрительнымъ и онъ донесъ, куда слѣдуетъ. Вмѣсто ожидаемаго воровского притона или т. п. нашли типографію; что же погубило ее: случайность или непростительная оплошность? Нельзя назвать случайнымъ арестъ ремингтона въ Петербургѣ въ концѣ 90-хъ годовъ, вызванный тѣмъ, что вниманіе жильцовъ было привлечено страннымъ ритмическимъ стукомъ по ночамъ, или арестъ Гольденберга въ Елизаветградѣ вслѣдствіе обратившаго на себя вниманіе своей относительной тяжестью чемодана съ динамитомъ, или аресты въ Бѣлостокѣ въ 1896 году, причиной которыхъ послужило то, что хозяинъ квартиры заподозрилъ въ своемъ часто запиравшемся съ гостями жильцѣ—фальшиваго монетчика, или арестъ одного товарища въ Витебскѣ, вызванный тѣмъ, что горничная, увидавъ въ рукахъ постового городового свѣжій гектографированный листокъ, сказала съ пренебреженіемъ: „Эка важность! Мой баринъ самъ ихъ дѣлаетъ". Во всѣхъ этихъ и въ тысячахъ другихъ аналогичныхъ случаевъ въ основѣ всегда лежитъ болѣе или менѣе грубый промахъ или недосмотръ со стороны революціонера-дѣятеля. Ужъ если говорить о случайностяхъ, то правильнѣе будетъ отнести къ этой категоріи тѣ „противоестественныя" явленія, когда мы *спасаемся* изъ бѣды *вопреки* оплошности. Идетъ, напр., Х. по улицѣ, нагруженный литературой; вдругъ у него лопается тесемка и часть книгъ вываливается; случайность будетъ, если подошедшій городовой любезно поможетъ ему собрать книжки, а не тогда, если раба божьяго отведутъ въ участокъ. Или У. отправляется сдавать литературу малой скоростью; пріемщикъ долго смотритъ на странный ящикъ, котораго удѣльный вѣсъ, характеръ упаковки не соотвѣтствуютъ обозначенному роду товара, качаетъ головой; однако, изъ лѣни пропускаетъ его благополучно. Вотъ такіе-то благополучные исходы изъ скверныхъ положеній, возникшихъ вслѣдствіе безпечности, можно дѣйствительно считать рѣдкими случайностями.

Несмотря на то, что борьба съ самодержавіемъ ведется не со вчерашняго дня, россійскій революціонеръ далеко еще не освободился отъ той „шири" и „размашистости" „русской натуры", которыя не могли считаться безразличными даже въ періодѣ „кружковщины", но безусловно вредны теперь, въ эпоху массоваго рабочаго движенія. Россійскому революціонеру суровыя требованія конспираціи, осторожности, а, главное, выдержки, все еще кажутся невыполнимыми, стѣснительными, тормозящими живое дѣло. Сплошь и рядомъ осторожность объявляется трусостью, отсутствіемъ настоящаго революціонизма и товарищескихъ чувствъ. Слова „авось", „небось", а—въ особенности—„сойдетъ!" то и дѣло приходится слышать. Мало того, осторожность даже объявляется несовмѣстимой со смѣлостью и рѣшительностью, что, само собою, ужъ совсѣмъ нелѣпо.

Много вреда приносятъ себѣ и другимъ тѣ товарищи, которые хотя знаютъ объ окружающихъ ихъ опасностяхъ, хотя видятъ зловѣщіе симптомы, показывающіе, что дѣло обстоитъ не совсѣмъ ладно, — однако безпечно машутъ рукой, утѣшаясь легкомысленнымъ „сойдетъ". Но еще во много разъ вреднѣе тотъ сортъ людей, которые ни о чемъ не задумываются, никакихъ опасностей не видятъ и дѣйствуютъ съ поразительной беззаботностью и младенческимъ невѣдѣніемъ. Надо употребить всѣ усилія, чтобы оба эти типа „дѣятелей" поскорѣе у насъ вывелись.

II. „ЛЕГАЛЬНОЕ“ ПИСЬМО.

Будь остороженъ. Почта, знаю,
Имѣетъ тайные приказы.
Шиллеръ, „Донъ Карлосъ“.

Какъ можетъ онъ оправдываться? Вотъ
Его письмо. О, ясно преступленье,
Какъ божій день!
Шиллеръ, „Марія Стюартъ“.

Знаменитый сатирикъ Салтыковъ начинаетъ одно изъ своихъ „Писемъ къ тетенькѣ“ сообщеніемъ, что вслѣдствіе пропажи послѣднихъ его писемъ онъ отправился за разъясненіями къ одному знакомому почтовому чиновнику, отъ котораго получилъ такой отвѣтъ: „Которыя письма не нужно, чтобы доходили, тѣ всегда у насъ пропадаютъ“. Конечно, въ данномъ случаѣ, это „эзоповскій“ оборотъ рѣчи: дѣло идетъ не о почтовыхъ письмахъ, а о печатныхъ статьяхъ, и не о почтѣ, а о цензурѣ. Однако, это даетъ ему поводъ коснуться и переписки.

„Вообще,—пишетъ онъ,—я нынче о многомъ сызнова передумываю, а между прочимъ и о томъ: отчего наши письма отъ времени до времени не доходятъ по адресу? И знаете ли, къ какому заключенію я пришелъ:—сами мы во всемъ виноваты! Письма надо писать кратко и складно, чтобы сразу можно было понять, въ чемъ суть, а мы пишемъ пространно и нескладно; въ письмахъ надобно излагать лишь нужные предметы, а остальное посвящать родственнымъ изліяніямъ, а мы наши письма наполняемъ околичностями, а объ родственныхъ чувствахъ умалчиваемъ. Вотъ какъ по настоящему надо писать:

„Милая тетенька! Я, слава Богу, живъ и здоровъ, чего и вамъ отъ души желаю!! Вчера былъ день рожденія покойнаго дяденьки, и я надѣюсь, что вы провели оный въ молитвѣ. Но отчаяваться однако же не слѣдуетъ, а надо помнить, что мы не для сего рождены!! Живите—не бойтесь! Но, главное, старайтесь находиться въ мирѣ съ сосѣдями. Потому что все это свѣдущіе люди. И я тоже живу, не боюсь, но стараюсь быть въ ладу съ дворниками и, слава Богу, веду себя, кажется, хорошо!! На дняхъ призывалъ меня нашъ околодочный и говоритъ: вы такъ хорошо себя ведете, что заслуживаете публичной похвалы!! Въ чемъ же, говорю, оная похвала будетъ состоять?! Однако же онъ не открылъ, а только усмѣхнулся и молвилъ: лучше, какъ сами своевременно сей сюрпризъ узнаете, и не велѣлъ отлучаться изъ дома, дабы похвалы не прозѣвать. И я сижу теперь въ ожиданіи!!! Братьямъ и сестрицамъ потрудитесь передать мой сердечный привѣтъ: я думаю, выросли. А у насъ все благополучно, только говядина сильно вздорожала, такъ что вынуждены мы съ симъ продуктомъ обходиться осторожно. Вообще, у кого аппетитъ хорошъ, тотъ долженъ нынѣ или сокращать оный, или же стараться, какъ можно чаще въ гостяхъ обѣдать. Но тогда тѣ, къ коимъ начнемъ „запросто“ учащать, могутъ вознегодовать. Затѣмъ, цѣлуя вамъ ручки, остаюсь любящій васъ племянникъ“ и т. д. „Въ такомъ видѣ, заключаетъ онъ, письмо навѣрное ни въ огнѣ не сгоритъ, ни въ водѣ не потонетъ, а такъ-таки цѣлехонькое и дойдетъ по адресу“.

Этотъ юмористическій образчикъ эзоповскаго письма и совсѣмъ не шуточное предупрежденіе насчетъ необходимости писать „складно“, во избѣжаніе пропажи писемъ, были напечатаны въ 1881 г., т. е. болѣе 20 лѣтъ тому назадъ. За этотъ періодъ россійское правительство не стало большимъ поклонникомъ принципа неприкосновенности частной переписки. Помимо гоголевскихъ Шпекиныхъ, вскрывающихъ и по сію пору въ менѣе крупныхъ почтовыхъ пунктахъ письма „любознательности“ ради, существуютъ повсюду „черные кабинеты“, гдѣ систематически пересматривается переписка и задерживается подозрительная. Въ извѣстные моменты опредѣленныя категоріи почтовыхъ отправленій подвергаются особенно тщательному осмотру. Напр., появленіе „Искры“, а потомъ „Освобожденія“, разсылавшихся изъ-за границы въ конвертахъ, заставило обратить усиленное вниманіе на заграничныя письма: начавшаяся агитація въ деревнѣ и разсылка нелегальныхъ изданій по почтѣ сельскимъ жителямъ вызвала изданіе секретныхъ циркуляровъ волостнымъ правленіямъ вскры-

вать всѣ письма, адресованныя въ деревни; лѣтомъ 1902 г. Плеве издалъ секретный циркуляръ также и для Финляндіи о вскрываніи писемъ въ присутствіи адресата, въ виду того, что „неблагонадежныя лица пользуются почтой для распространенія періодическихъ изданій и другихъ произведеній печати противоправительственнаго содержанія“. Если, тѣмъ не менѣе, огромный процентъ нелегальныхъ писемъ проскальзываетъ благополучно, то это объясняется, съ одной стороны, тѣми предосторожностями, которыя принимаются революціонерами какъ въ отношеніи адресатовъ, такъ и содержанія письма, а съ другой стороны — и это гораздо важнѣе — полной невозможностью вскрывать и внимательно изслѣдовать колоссальное количество ежедневно протекающей корреспонденціи (до 600 милліоновъ въ годъ), безъ непомѣрнаго увеличенія чиновъ сыска и безъ такой продолжительной задержки корреспонденціи, которая отразилась бы гибельно на всей промышленности и вызвала бы безконечныя жалобы. Вскрываются поэтому лишь тѣ почтовыя отправленія, которыя почему-либо выдѣляются изъ ряда остальныхъ и кажутся подозрительными, напримѣръ, если адресатъ завѣдомо „неблагонадежный“, а то и поднадзорный человѣкъ, или если онъ просто принадлежитъ къ „интеллигентнымъ“ профессіямъ, внушающимъ къ себѣ мало довѣрія (студенты, акушерки, дантисты, курсистки, статистики и т. д.); въ особенности же задерживаются тѣ письма, которыя обращаютъ на себя вниманіе своимъ объемомъ, толщиной, прощупываемымъ внутреннимъ конвертомъ, или, наконецъ, тѣ, на адресѣ которыхъ есть приписка „для N“. Если по вскрытіи не оказывается ничего подозрительнаго, то оно вновь заклеивается и доставляется по назначенію (а то и просто уничтожается — стоитъ ли церемониться!); въ противномъ же случаѣ возбуждается дѣло. Очень часто жандармы, снявъ копію съ письма (если оно „легальное“, т. е. безъ „химіи“), отсылаютъ его по адресу и потомъ либо въ ту же ночь являются съ обыскомъ, либо учреждаютъ шпіонскій надзоръ, чтобы добыть новыя нити. Что считается подозрительнымъ въ письмахъ — это часто зависитъ отъ усмотрѣнія жандарма. Въ одномъ случаѣ, напр., былъ произведенъ рядъ обысковъ потому, что въ перехваченномъ письмѣ заключалась просьба уничтожить письмо по прочтеніи. Въ другомъ — была по телеграфу задержана посылка и явившіеся за ней, потому что въ одномъ изъ вскрытыхъ на почтѣ писемъ находилась просьба не распечатывать посылку при постороннихъ (къ большому конфузу жандармовъ въ посылкѣ оказалось обыкновенное мужское бѣлье, которое невѣста посылала своему жениху въ подарокъ). Когда-то Пушкинъ былъ сосланъ на нѣсколько лѣтъ въ село Михайловское вслѣдствіе перехваченнаго на почтѣ письма его, гдѣ находилась такая „ужасная“ фраза: „беру уроки чистаго аѳеизма... система не столь утѣшительная, какъ думаютъ, но къ несчастью болѣе всего правдоподобная“. Теперь времена иныя; „аѳеизмъ“ отошелъ на послѣдній планъ, но соотношеніе между незначительностью вызывающихъ подозрѣніе фразъ и вызываемыми ими крупными послѣдствіями зачастую остается такимъ же.

Вторымъ источникомъ захвата письменныхъ документовъ являются обыски. Казалось бы, что въ странѣ, гдѣ сложилась народная пословица: „отъ тюрьмы да отъ сумы не отрекайся“, гдѣ рѣшительно никто не гарантированъ отъ обысковъ, должна была бы выработаться привычка не держать у себя компрометирующихъ бумагъ: тѣмъ не менѣе, въ этомъ отношеніи наблюдается самая вопіющая небрежность. Основное правило гласитъ: „уничтожайте *всякое*, полученное вами, письмо сейчасъ же по прочтеніи или использованіи“, хотя бы оно было совершенно невинное. Зачѣмъ сохранять у себя интимныя письма? Не затѣмъ ли, чтобы жандармы перебирали ихъ своими грязными руками, отпускали по нимъ замѣчанія и знали вашихъ знакомыхъ? Если же въ письмѣ есть хоть малѣйшій намекъ, могущій скомпрометировать адресата или другихъ лицъ, или устанавливающій связь между ними, — то хранить такое письмо — есть преступленіе. Уничтожать каждое полученное письмо — одно изъ первыхъ обѣщаній, обязательное для всякаго лица, съ которымъ организація имѣетъ хоть малѣйшія сношенія. Сколько проваловъ было вызвано отобранными при обыскахъ документами — трудно себѣ и представить. Въ нихъ для жандармовъ пріобрѣтаетъ значеніе каждая мелочь, каждая черточка. Во-первыхъ, они получаютъ неопровержимое свидѣтельство о знакомствѣ лицъ, хотя бы только автора и адресата: почеркъ, подпись, тонъ письма наводятъ на опредѣленные выводы, хотя бы лицо, у котораго оно найдено, не давало никакихъ разъясненій. Во-вторыхъ, еще важнѣе заключающіяся въ немъ указанія на знакомства другихъ лицъ и на различныя событія или обстоятельства.

Выше мы сказали, что обѣщаніе уничтожать письма по прочтеніи слѣдуетъ брать со *всякаго* человѣка, съ которымъ такъ или иначе сталкивается организація. Это можетъ показаться страннымъ, но дѣло въ томъ, что и маленькіе люди своей перепиской могутъ вредить и дѣйствительно вредятъ крупному дѣлу. Въ каждомъ городѣ, гдѣ есть революціонное движеніе (а гдѣ въ настоящее время такого нѣтъ?), въ периферіи организаціи ютится болѣе или менѣе широкій контингентъ юношей и дѣвицъ, такъ или иначе соприкасающихся съ личностями, входящими въ организацію. Од и изъ нихъ участвуютъ въ кружкахъ подъ чьимъ-нибудь руководствомъ, другіе оказываютъ различныя услуги, собирая деньги, доставляя адреса, вещи для пересыльныхъ; наконецъ, третьи просто сталкиваются съ людьми организаціи въ домахъ общихъ знакомыхъ, либеральныхъ или индифферентныхъ. Изъ этого контингента лицъ въ дальнѣйшемъ настоящіе, преданные революціонеры выходятъ въ небольшомъ числѣ; остальные скоро сбрасываютъ или припрятываютъ модное платье и превращаются въ либераловъ, или просто коптителей неба, а то и въ торжествующихъ поросятъ. Между тѣмъ, у каждаго имѣется гдѣ-нибудь въ другомъ городѣ подруга, товарищъ, другъ сердца, женихъ или невѣста, которымъ аккуратно, съ трогательной непосредственностью, сообщается все, до мельчайшихъ подробностей. Если особа посѣщаетъ кружокъ, то сообщается о томъ, кто остальные участники, кто лекторъ, что читается и т. д. Если она сотрудничаетъ въ библіотечкѣ, отдѣленіи Краснаго Креста, встрѣчается съ рабочими, то обо всемъ этомъ считается долгомъ (не скрывать же такихъ вещей отъ закадычнаго друга!) сообщать въ письмахъ подробнѣйшимъ образомъ. Приведу для примѣра нѣсколько истинныхъ происшествій. Одинъ студентъ писалъ другому, что онъ вмѣстѣ съ 5-ю другими составилъ „кружокъ саморазвитія", гдѣ читаютъ „Капиталъ" Маркса. Письмо было перехвачено, были произведены обыски, допросы и т. д. Ни малѣйшаго состава преступленія нельзя было найти, и все вошло въ обычную колею. Но когда наступили вакаціи, и студенты разъѣхались по домамъ, то всѣ 6 участниковъ „преступнаго" кружка получили черезъ полицію обратно свои документы, дескать, намъ такихъ студентовъ не надо. Тутъ, по крайней мѣрѣ, не пострадала никакая революціонная организація. А вотъ другой случай: дѣвица пишетъ своей пріятельницѣ и, между прочимъ, сообщаетъ, что у нихъ въ городѣ появился интересный человѣкъ (имя рекъ), соціалдемократъ, и теперь стало оживленнѣе. Адресатка письмо, конечно, сохранила у себя. Черезъ много мѣсяцевъ жандармерія почему-то пожаловала къ ней съ обыскомъ, нашла письмо и заинтересовалась иногороднимъ „интереснымъ человѣкомъ". По телеграфу отдано было распоряженіе произвести у него обыскъ. Тамъ, по несчастью, гостилъ проѣздомъ одинъ видный членъ организаціи, при которомъ находилось много сильно компрометирующихъ его документовъ. Въ связи съ ними было забрано еще нѣсколько человѣкъ, и все это надѣлало гл пое письмо наивной дѣвицы, сохранявшееся другой наивной дѣвицей.

Вотъ почему слѣдуетъ быть крайне осторожнымъ въ сношеніяхъ съ незрѣлой, неопытной молодежью и тщательно ей внушать элементарныя правила конспираціи. Не нужно смущаться тѣмъ, что такіе совѣты часто принимаются ими за личную обиду, а нужно долбить да долбить, уличать въ неисполненіи правилъ и, убѣдившись въ безнадежности „науки", какъ можно скорѣе прервать всякія сношенія съ ними.

Есть, однако, компрометирующіе документы, которые, по ихъ характеру, поневолѣ приходится нѣкоторое время у себя сохранять, и которые, слѣдовательно, могутъ при обыскѣ попасть въ руки жандармовъ; таковы — списки адресовъ *) и различныя рукописи: статьи, корреспонденціи, наброски прокламацій, протоколы, программы и т. п. Здѣсь на первый планъ выдвигается почеркъ. Во всѣхъ „дѣлахъ" жандармскихъ управленій экспертиза каллиграфовъ играетъ огромную роль, и много сотенъ политическихъ попали въ ссылку исключительно на основаніи констатированнаго сходства ихъ почерка съ тѣмъ, которымъ писаны захваченныя у нихъ самихъ или другихъ бумаги. Отрицаніе въ такихъ случаяхъ ни къ нему не ведетъ, хотя, надо сказать, каллиграфы часто допускаютъ возмутительныя ошибки. Поэтому всякій, пишущій что-либо нелегальное, долженъ всегда помнить, что онъ создаетъ такимъ образомъ неопровержимое прямое свидѣтельство своей революціонной дѣятельности. Если шансовъ того, что рукопись попадется, и что почеркъ будетъ узнанъ, мало.

*) О нихъ, какъ и о многихъ другихъ вопросахъ, связанныхъ съ перепиской, рѣчь будетъ въ XXI главѣ.

напр., если она сдается прямо въ типографію для немедленнаго напечатанія или увозится заграницу либо въ какой-нибудь отдаленный городъ, то допустимо еще писать своимъ почеркомъ. Въ противномъ случаѣ должно прибѣгнуть къ какимъ-нибудь мѣрамъ; такихъ можно указать три: 1) поручить переписать рукопись другому лицу, стоящему далеко отъ движенія и, во всякомъ случаѣ, не могущему никакъ быть заподозрѣннымъ, какъ авторъ статьи; 2) писать „печатными" буквами, и 3) писать измѣненнымъ почеркомъ. Первый способъ далеко не часто можно примѣнять: требованія конспираціи не позволяютъ давать статью или другіе документы человѣку, не стоящему достаточно близко къ организаціи; дать же активному члену — значитъ только переложить рискъ съ одного на другого. Писать „печатными" буквами можно легко научиться; распознать почеркъ въ этомъ случаѣ почти или вовсе невозможно, но это требуетъ очень много времени и терпѣнія. Поэтому, такой способъ примѣнимъ только къ сравнительно небольшимъ текстамъ. Онъ обязателенъ: во всѣхъ письмахъ, прокламаціяхъ, протоколахъ и тому подобныхъ небольшихъ документахъ, пересылаемыхъ оказіей (см. гл. XXI); въ корреспонденціяхъ, посылаемыхъ по почтѣ заграницу; въ тюремной перепискѣ (см. гл. XXI); въ замѣткахъ, дѣлаемыхъ на поляхъ нелегальныхъ книгъ, и въ поправкахъ на печатномъ текстѣ; въ небольшихъ документахъ, которые приходится держать при себѣ или возить съ собой.

Во всѣхъ остальныхъ случаяхъ остается писать измѣненнымъ почеркомъ — совѣтъ, о которомъ можно сказать: могущій вмѣстить, да вмѣститъ. Дѣло въ томъ, что до сихъ поръ не изобрѣтены, къ сожалѣнію, такіе способы, помощью которыхъ можно было бы каждому измѣнять свой почеркъ до неузнаваемости. Мы можемъ только дать такой совѣтъ. Каждый революціонеръ, которому приходится много писать, долженъ выработать себѣ „нелегальный" почеркъ. Многія буквы русской азбуки пишутся нѣсколькими варіаціями: д, з, л, т, Б, В, ѣ, и т. д.; тѣ начертанія, которыхъ онъ не употребляетъ въ нормальномъ своемъ письмѣ, онъ долженъ усвоить для нелегальнаго; равнымъ образомъ и остальные буквы онъ долженъ видоизмѣнить, для чего лучше всего взять за образецъ какой-нибудь автографъ — рѣзко отличный отъ его собственнаго; далѣе, если онъ вообще пишетъ косыми буквами и слитно, то онъ долженъ научиться писать прямыми и расчлененными буквами (безъ соединенія штрихами); если онъ пишетъ тонко, пусть беретъ мягкое перо. Если онъ надъ всѣмъ этимъ поупражняется нѣкоторое время, то у него выработается почеркъ, совершенно непохожій на его собственный. Онъ долженъ только стараться не смѣшивать ихъ между собой, т. е. легальныя вещи обязательно писать обыкновеннымъ почеркомъ, а прочія обязательно нелегальнымъ. Сказанное относится не только къ буквамъ, но и къ цифрамъ.

Если письма сейчасъ же по полученіи уничтожаются, то почти единственный путь для нихъ попасть въ руки жандармовъ — быть захваченными на почтѣ. Если адресъ вѣрный, если письмо по внѣшнему виду не подозрительно, то шансы для его вскрытія небольшіе; если, будучи все же вскрыто, оно не содержитъ никакихъ подозрительныхъ вложеній и писано естественнымъ почеркомъ, то благополучное его прохожденіе зависитъ исключительно отъ содержанія. Спрашивается, можно ли писать о нелегальныхъ вещахъ легальнымъ способомъ? Безъ сомнѣнія, относительно многихъ вещей отвѣтъ можетъ быть утвердительный — надо только писать въ замаскированномъ, условномъ, „эзоповскомъ" стилѣ. Такія весьма важныя и часто спѣшныя сообщенія, какъ объ обыскахъ, арестахъ, демонстраціяхъ, стачкахъ, полученіи литературы и потребности въ ней, выходѣ новыхъ номеровъ періодическихъ изданій, полученіи денегъ и высылкѣ таковыхъ, перемѣнѣ адреса, отзывы о литературѣ, сообщенія о скоромъ пріѣздѣ и т. д. — могутъ заключаться и въ обыкновенномъ „легальномъ" письмѣ. Выраженныя иносказательно, они должны тонуть въ остальномъ содержаніи; они должны представлять невинныя вкрапленія въ невинномъ текстѣ. Такъ какъ они нерѣдко бываютъ такъ искусно скрыты, что обманываютъ самого чтеца, который принимаетъ ихъ за чистую монету, то во избѣжаніе этого требуется раньше дать намекъ, что дальше начинается „эзоповщина". Это достигается, напр., тѣмъ, что корреспондентъ приписываетъ получателю такое дѣйствіе, котораго онъ не дѣлалъ. Напримѣръ, послѣ обычныхъ привѣтствій и т. п. идетъ такой отрывокъ: „...Къ сожалѣнію, я не могъ исполнить твоей просьбы заказать для тебя еще дюжину карточекъ. Фотографія, гдѣ ты снималась, и о которой ты мнѣ писала, не существуетъ болѣе. Дѣла тамъ шли плохо, имущество описали, хозяинъ съ женой скрылись. Придется тебѣ вновь сниматься: помни, что ты давно мнѣ обѣщала подарить

свою карточку" и т. д. Авторъ письма, конечно, никакой просьбы заказать карточки не получилъ; его корреспондентъ сейчасъ же догадывается, что дальше начинается иносказаніе и на основаніи извѣстныхъ ему свѣдѣній соображаетъ, что провалилась типографія, а работавшимъ въ ней удалось скрыться.

Считаемъ нелишнимъ напомнить, что нѣкоторыя иносказательныя выраженія (напр., „блины" вмѣсто „прокламаціи" и „заболѣлъ" вмѣсто „арестованъ") слишкомъ ужъ затасканы и общеизвѣстны, поэтому должны быть замѣнены другими *).

О демонстраціяхъ, стачкахъ, открытыхъ собраніяхъ, крупныхъ сенсаціонныхъ провалахъ, распространеніи прокламацій и т. п. общеизвѣстныхъ въ данномъ мѣстѣ вещахъ можно писать открыто, освѣщая ихъ съ точки зрѣнія добродѣтельнаго бюргера, возмущеннаго продѣлками безпокойныхъ бунтовщиковъ.

Однако, построить дѣловую революціонную переписку на „легальныхъ" письмахъ невозможно. Лишь только надо выразиться опредѣленнѣе, напр., вмѣсто простой просьбы о присылкѣ литературы, указать точно, какую именно и въ какомъ числѣ экземпляровъ, когда нужно сообщить новый адресъ, разсказать подробности проваловъ, условиться относительно какого-нибудь конспиративнаго дѣла, то эзоповскій методъ совершенно непригоденъ. Приходится писать ясно и точно, чтобы не было ни недоразумѣній, ни сомнѣній. И въ то же время надо писать такъ, чтобы самый зоркій и проницательный взоръ жандарма не могъ добраться до смысла написаннаго. Эта задача разрѣшается *шифромъ*.

III. ГИБЕЛЬНЫЙ САМООБМАНЪ.

Лишь самъ себя обманомъ не тѣши,
Теперь никто тебя ужъ не обманетъ!
Гете, „Торквато Тассо".

...Черезъ нѣкоторое время сковородка сильно нагрѣлась; тогда я повернулъ листокъ и къ невыразимой своей радости замѣтилъ на немъ какія-то фигурки, расположенныя строчками...
Эдгаръ Поэ, „Золотой жукъ".

Съ понятіемъ „шифръ" у всякаго обывателя, не исключая большинства революціонеровъ, связывается представленіе о чемъ-то весьма хитромъ, неразрѣшимомъ, таинственномъ. Послать шифрованное письмо—это значитъ заключить свои слова въ такую броню, раздробить которую никому не удастся, кромѣ посвященнаго, обладающаго ключемъ. При взглядѣ на ряды каббалистическихъ знаковъ, буквъ, цифръ, предъ которыми стоишь совершенно безпомощнымъ, если не являешься избранникомъ изъ $1^1/_2$ милліардовъ обитателей земного шара, поневолѣ проникаешься чувствомъ благоговѣйнаго почтенія. Прочтите, напр., сцену изъ романа Степняка „Андрей Кожуховъ" (часть I, глава I), изображающую, какъ Андрей заграницей нагрѣваетъ и читаетъ шифрованное письмо, только что полученное изъ Россіи, и вы убѣдитесь, что и герой романа Андрей, и авторъ вполнѣ увѣрены, что тѣ чрезвычайно секретныя вещи, о которыхъ сообщалось въ письмѣ, никоимъ образомъ не могли бы стать извѣстными Департаменту Полиціи, даже если бы письмо очутилось у него въ рукахъ. Вѣра въ шифръ дѣйствительно замѣчательна въ русскомъ революціонерѣ. Болѣе 99% писемъ, которыми революціонеры обмѣниваются, шифрованныя; они отправляются съ самой спокойной душой; имъ довѣряютъ самыя важныя тайны. Сколько надо имѣть

*) Здѣсь умѣстно будетъ обратить вниманіе на ту подозрительность, какую иногда проявляютъ жандармы при чтеніи перехваченныхъ ими легальныхъ писемъ, принимая въ нихъ самыя невинныя выраженія за таинственныя иносказанія. Такъ, въ Смоленскѣ они долго искали въ 1902 году мастерскую взрывчатыхъ веществъ, на основаніи слѣдующаго мѣста въ перехваченномъ ими письмѣ: „Какъ идутъ дѣла въ вашей мастерской, расширили ли вы ее" и т. д. Рѣчь шла объ обыкновенной мастерской.

вѣры въ шифръ, чтобы хранить у себя съ полнѣйшимъ спокойствіемъ списки зашифрованныхъ адресовъ, т. е. судьбу многихъ лицъ!

Писать шифромъ — вещь, несомнѣнно, хлопотливая. Однако, хлопотливость шифрованной переписки и всѣ связанныя съ ней затрудненія искупаются для революціонеровъ громаднымъ значеніемъ ея, какъ оборонительнаго оружія.

Въ самомъ дѣлѣ, въ какомъ трудномъ, безпомощномъ положеніи очутились бы мы безъ такого оружія. Чѣмъ многочисленнѣе становятся гнѣзда революціонной дѣятельности, тѣмъ сношенія по необходимости должны дѣлаться все чаще и систематичнѣе. Они могутъ быть двухъ родовъ: устныя и письменныя. Если въ XVI-мъ вѣкѣ флибустьеръ протестантскихъ войнъ Морицъ Саксонскій держался того мнѣнія, что „изустный разговоръ или обмѣнъ мыслей гораздо лучше, чѣмъ писанная бумага", то уже злой пародіей звучитъ у Тургенева, когда онъ разсказываетъ въ 70-хъ годахъ, что „Матурину, которая едва знала по-нѣмецки, посылали въ Женеву для того, чтобы вручить тамъ неизвѣстному ей лицу половину куска картона съ нарисованной виноградной вѣткой и 279 рублей серебра". Въ настоящее время личныя сношенія для устныхъ ли разговоровъ или для врученія „картоновъ" сдѣлались не только крайне опасными, но въ большинствѣ случаевъ невозможными. Государственная почта—вотъ кто долженъ поддерживать сношенія между революціонными организаціями, какъ государственныя желѣзныя дороги развозятъ нелегальную литературу. Но довѣрять правительственной почтѣ наши тайны, если бы они не были защищены шифромъ, было бы безуміемъ.

Однако, на чемъ основана наша вѣра въ неразрѣшимость шифра? Что, если мы ошибаемся? если тайна, довѣренная шифру, ужъ не тайна? если мы все время пребываемъ въ состояніи автомистификаціи? если о всей нашей работѣ по составленію и разбору шифрованныхъ писемъ приходится сказать съ улыбкой сожалѣнія: „трудишься много ты, да пользы въ этомъ нѣтъ!" Какъ ни неожиданными могутъ показаться эти вопросы, однако они вполнѣ законны.

Основываясь на случаяхъ раскрытія писемъ бюро Департамента Полиціи и на нашемъ личномъ опытѣ, мы не только ставимъ вышеприведенный вопросъ о самообманѣ, но даемъ на него вполнѣ опредѣленный и категорическій *утвердительный* отвѣтъ: да, мы, россійскіе революціонеры, въ отношеніи шифровъ пребываемъ въ состояніи самаго вреднаго самообмана. Мы похожи на того короля, который разгуливалъ голый по городу, увѣренный, что на немъ пышное платье. И намъ, и нѣкоторымъ товарищамъ нашимъ приходилось иногда поневолѣ предпринимать попытки раскрывать письма безъ ключа. Это случалось тогда, когда корреспондентъ перепутывалъ ключъ, или, если въ отсутствіи товарища, обыкновенно ведшаго переписку, получалось письмо изъ такого города, для котораго тотъ позабылъ сообщить ключъ. И что же? Не было ни одного случая, когда бы шифръ оставался неразобраннымъ. Въ данный моментъ это обстоятельство было, положимъ, пріятно, но оно заставляло сильно и сильно призадумываться. Для чего же въ самомъ дѣлѣ разводить канитель, трудиться, заставлять трудиться другихъ, когда это отнюдь не спасаетъ?

Занявшись этимъ вопросомъ, мы пришли къ такому заключенію: подавляющее большинство шифрованныхъ писемъ, которыми обмѣниваются наши товарищи, весьма легко могутъ быть раскрыты; *ни одна* изъ употребляющихся системъ не можетъ быть названа удовлетворительной; чуть ли не всѣ товарищи, безъ исключенія, обнаруживаютъ непониманіе тѣхъ законовъ, на которыхъ основывается разгадка шифровъ, и тѣхъ пріемовъ, которыми можно сдѣлать ее невозможной. Въ то же время мы убѣдились, что возможны и хорошія, надежныя системы, возможно и разумное отношеніе къ дѣлу, возможно, однимъ словомъ, писать письма, которыхъ раскрыть не удастся. Мы поэтому рѣшили разобрать здѣсь всѣ употребляющіяся у насъ системы, съ которыми намъ приходилось сталкиваться, представить по каждой примѣрный образчикъ методическаго раскрытія, ибо только такимъ образомъ слабыя стороны каждой системы выступятъ настолько ясно, что отобьютъ всякую охоту впредь ею пользоваться.

Въ виду важности этихъ примѣрныхъ разборовъ, мы считаемъ нужнымъ сказать нѣсколько словъ относительно *текстовъ* для тѣхъ „задачъ", которыя мы подвергали анализу. Для успѣшнаго раскрытія шифра огромное значеніе имѣетъ *размѣръ* текста, ибо въ очень малыхъ криптограммахъ ни фонетическіе законы, ни особенности системы не могутъ проявиться достаточно рельефно. Если не всѣ попадавшія въ бюро письма расшифровывались, то это, вѣроятно, исключительно объясня-

ется малымъ количествомъ буквъ*). Наши примѣрные тексты колеблются въ предѣлахъ между 64 и 470 буквами, въ среднемъ около 180 буквъ. Въ обычныхъ письмахъ количество зашифрованныхъ буквъ рѣдко меньше означеннаго числа, часто оно бываетъ значительно больше, доходя до 1000 — 2000 буквъ. Къ тому же мы брали сплошные тексты, а это представляетъ бо́льшія трудности. Во всѣхъ задачахъ мы совершенно исключили методъ „пробъ" и угадыванія, хотя на практикѣ онъ играетъ огромную роль въ дѣлѣ раскрытія. Но онъ слишкомъ субъективенъ и потому не убѣдителенъ и для нашей дидактической цѣли не годится.

Тексты мы заимствовали изъ первыхъ попавшихся подъ руку книгъ. Ключи мы старались брать — тамъ, гдѣ отъ удачнаго подбора его много зависитъ (какъ напр., въ квадратныхъ системахъ) — возможно ближе къ максимуму достижимаго**).

Прежде, однако, чѣмъ перейти къ анализу системъ шифровъ, намъ нужно сдѣлать небольшую экскурсію въ область русской фонетики.

---

*) Кромѣ, впрочемъ, тѣхъ случаевъ, когда шифровали по книгѣ или стихотворенію (см. гл. XV и XVI).

**) Первый вопросъ, который приходится разрѣшать, сталкиваясь съ зашифрованнымъ текстомъ — это вопросъ о языкѣ, такъ какъ принципы рѣшенія опредѣляются особенностями языка. Обыкновенно начинаютъ дешифрированіе съ русскаго языка, но это не всегда ведетъ къ цѣли, такъ какъ на окраинахъ возможно употребленіе въ шифрованныхъ письмахъ какого-нибудь другого языка (польскаго, еврейскаго, армянскаго, грузинскаго и пр.). Мы здѣсь ограничивались исключительно русскимъ языкомъ.

Глава I.

НЕМНОЖКО ФОНЕТИКИ. КЛАССИФИКАЦІЯ ШИФРОВЪ.

Міръ не чудитъ. Всему въ немъ есть
Свои законы, вѣсъ и мѣра.
Жемчужниковъ.

Послѣ *онъ* слѣдуетъ тотчасъ *покой;*
Въ азбукѣ нашей порядокъ такой.
Шиллеръ, „Лагерь Валленштейна".

Прежде чѣмъ взяться за разборъ разнообразныхъ системъ шифровъ, намъ придется сдѣлать небольшую экскурсію въ область фонетики русскаго языка, такъ какъ на законахъ ея основываются способы раскрытія почти всѣхъ шифровъ. Какъ живой, естественный продуктъ исторической жизни народа, языкъ подчиненъ ряду законовъ, проявляющихся не только въ грамматикѣ и словообразованіи, но и фонетикѣ. Русская азбука содержитъ въ себѣ, какъ извѣстно, 36 буквъ, въ томъ числѣ двѣ конечныя ѳ и ѵ, почти совершенно неупотребительныя. За вычетомъ этихъ двухъ буквъ, которыя всегда игнорируются корреспондентами, остальныя 34 буквы располагаются въ слѣдующемъ порядкѣ:

Таблица № 1.

1, а	7, ж	13, л	19, с	25, ч	31, ѣ
2, б	8, з	14, м	20, т	26. ш	32, э
3, в	9, и	15, н	21, у	27, щ	33, ю
4, г	10, і	16, о	22, ф	28, ъ	34, я
5, д	11, й	17, п	23, х	29, ы	
6, е	12, к	18, р	24, ц	30, ь	

Мы помѣстили букву *й* послѣ і, но нѣкоторые помѣщаютъ ее въ концѣ алфавита. Часто выбрасываются тѣ или другія буквы, которыя считаются излишними. Этой участи подвергаются обыкновенно і, й, ъ, ь, ѣ, э, ы, либо всѣ, либо часть ихъ. Понятно, что въ такихъ случаяхъ необходимо уславливаться объ этомъ заранѣе. Если это забываютъ дѣлать, то выходитъ нерѣдко путаница, и малоопытные получатели криптограммы оказываются въ безпомощномъ положеніи. Поэтому разумнымъ является, когда хотятъ сократить алфавитъ, пользоваться такъ называемой „тюремной азбукой". Этимъ именемъ зовется извѣстнымъ образомъ расположенная *) азбука изъ 28 буквъ, служащая для перестукиванія въ тюрьмахъ. Въ ней буквы и ихъ порядокъ таковы:

Таблица № 2.

1, а	5, д	9, и	13, п	17, с	21, х	25, щ
2, б	6, е	10, к	14, о	18, т	22, ц	26, ы
3, в	7, ж	11, л	15, п	19, у	23, ч	27, ю
4, г	8, з	12, м	16, р	20, ф	24, ш	28, я

Насколько раціональна эта азбука, какъ и вообще идея сокращать азбуку, этого мы коснемся въ слѣдующихъ главахъ. Во избѣжаніе путаницы мы почти вездѣ пользовались и имѣли въ виду полную азбуку (Таблица № 1) и только въ нѣкоторыхъ случаяхъ, которые вездѣ оговаривали, мы считали нужнымъ примѣнить тюремную.

Основной фонетическій законъ касается частоты различныхъ буквъ въ русскомъ языкѣ. Во-первыхъ, однѣ буквы употребляются несравненно чаще другихъ, а, во-

*) Въ шесть рядовъ по пяти буквъ въ каждомъ. Шестой неполный. Подробнѣе о тюремныхъ сношеніяхъ мы говоримъ въ XXI главѣ.

вторыхъ, степень частоты каждой буквы есть нѣчто весьма постоянное. Мы нашли для русской азбуки слѣдующія числа:

Таблица № 3.

	На 1000 буквъ				
а	встрѣчается 75 разъ	і— 7	с—54	ъ—48
б	„ 20 „	й— 9	т—65	ы—20
в	„ 40 „	к— 29	у—23	ь—12
г	„ 12 „	л— 42	ф—0,1	ѣ—20
д	„ 32 „	м— 30	х— 8	э— 1
е	„ 66 „	н— 69	ц— 3	ю— 9
ж	„ 10 „	о—112	ч—13	я—19
з	„ 16 „	п— 25	ш— 4	
и	„ 66 „	р— 37	щ— 4	

Какъ извѣстно, ни одно царство природы не обходится безъ „царя", какъ ни одна область промышленности безъ „короля". Есть король и въ русской азбукѣ, и король этотъ—*о*. Его королевское достоинство не можетъ быть подвергнуто никакому сомнѣнію. Онъ рѣзко возвышается надъ остальными буквами своимъ коэффиціентомъ и, главное, никогда не уступаетъ другой буквѣ своего первенствующаго положенія. Онъ, однимъ словомъ, „большой король, хоть въ маломъ видѣ". Въ каждомъ языкѣ есть такіе короли: напр., въ нѣмецкомъ, французскомъ и англійскомъ—е, въ еврейскомъ—„алефъ". Для шифровъ это обстоятельство оказывается весьма пагубнымъ. Подобно коммунистическимъ обществамъ, они могутъ быть прочными только на базисѣ всеобщаго равенства. Если бы всѣ буквы встрѣчались въ языкѣ одинаково часто, врядъ ли можно было бы раскрыть хоть одинъ шифръ. Въ дѣйствительности же задача эта совсѣмъ нетрудная.

Для цѣли дешифрированія весьма полезно раздѣлить азбуку по частотѣ отдѣльныхъ буквъ на разряды. Мы дѣлимъ ихъ на пять разрядовъ, не считая буквы о, которую выдѣляемъ въ особый высшій или нулевой разрядъ.

Таблица № 4.

Высшій (нулевой) разрядъ—отъ 120 до 80; одна буква: о (коэффиціентъ 112).

Первый разрядъ—80 до 40; восемь буквъ: **а** (75), **н** (69); **е**, **и** (по 66), **т** (65), **с** (54), **ъ** (48), **л** (42).

Второй разрядъ—40 до 20; семь буквъ: **в** (40), **р** (37), **д** (32), **м** (30), **к** (29), **п** (25), **у** (23).

Третій разрядъ — 20 до 10; восемь буквъ: **б**, **ы**, **ѣ** (по 20), **я** (19), **з** (16), **ч** (13), **г**, **ь** (по 12).

Четвертый разрядъ—10 до 1; восемь буквъ: **ж** (10), **й**, **ю** (по 9), **х** (8), **і** (7), **ш**, **щ** (по 4), **ц** (3).

Пятый разрядъ—1 до 0; двѣ буквы: **э** (1), **ф** (0,1).

Въ этой табличкѣ буквы расположены по убывающей частотѣ. Самой рѣдкой буквой является *ф*, совершенно несвойственная русскому языку. Представляя противоположную крайность, и она играетъ предательскую роль. Всѣ приведенныя числа надо понимать, какъ среднія изъ нѣсколькихъ десятковъ случаевъ. Въ каждомъ индивидуальномъ случаѣ обязательно будутъ уклоненія, тѣмъ большія, чѣмъ меньше текстъ. Для нѣкоторыхъ буквъ размахи качанія довольно значительны (напр., для *а* отъ 50 до 90), для другихъ (напр., для *м*) весьма небольшія. Отъ такихъ уклоненій распредѣленіе буквъ по частотѣ отступаетъ отъ таблицы № 4; вмѣсто порядка: а, н, е, и, т, с, ъ, л... мы можемъ получить, напр., т, и, л, е, а, е, ъ, н... Однако, при всѣхъ этихъ измѣненіяхъ буквы обыкновенно не покидаютъ своихъ разрядовъ. Буква *о* всегда занимаетъ вершину; первыя восемь буквъ оказываются именно перворазрядными; развѣ только пограничная *в* ворвется въ первый разрядъ.

Дѣло дешифрированія весьма облегчается, если представить себѣ графически въ формѣ кривой частоту буквъ въ связи съ *мѣстомъ* ихъ въ алфавитѣ, какъ это сдѣлано нами на таблицѣ № 5*). Она намъ показываетъ, что азбука распадается на три рѣзко отличающихся другъ отъ друга *отдѣла*. Первый отдѣлъ (отдѣлъ буквы *а*, или

*) См. въ концѣ книги.

точнѣе отдѣлъ перворазрядныхъ гласныхъ) обнимаетъ 11 буквъ, отъ *а* до *й* включительно и графически представляетъ рядъ горныхъ вершинъ, перемежающихся глубокими долинами. Второй отдѣлъ (отдѣлъ буквы *о*, или центральный) обнимаетъ 10 буквъ отъ *к* до *у* включительно и представляетъ высокое плоскогоріе, на которой въ самой серединѣ гордо высится подобно Монблану—буква *о*. Такая почтенная свита, сгруппировавшаяся вокругъ нашего „короля", еще болѣе удостовѣряетъ, что это могущественный монархъ, „король отъ головы до пятокъ". Наконецъ. третій отдѣлъ (отдѣлъ рѣдкихъ буквъ) заключаетъ въ себѣ 13 буквъ отъ *ф* до *я* и на нашей кривой представляетъ низменность, на которой есть только одно порядочное возвышеніе—буквы *ъ*. Но такъ какъ эта буква почти никогда не употребляется въ шифрахъ, то срѣзавъ эту вершину, мы получаемъ видъ еще болѣе однообразный и пустынный. Такое любопытное распредѣленіе отдѣловъ оказываетъ при раскрытіи шифровъ весьма цѣнныя услуги, въ особенности это можно сказать о центральномъ отдѣлѣ. этомъ сплошномъ скопленіи частыхъ буквъ. Вверху таблицы 5 особо отмѣчены: *рядъ* а (т. е. десятокъ буквъ, начинающихся съ а), *рядъ* е, *рядъ* и, *рядъ* о. Это понадобится намъ при разборѣ квадратныхъ шифровъ.

Познакомивъ читателя съ основнымъ фонетическимъ закономъ, намъ остается лишь сдѣлать нѣсколько мелкихъ замѣчаній. Буква і ставится обязательно *передъ* гласной (кромѣ „міръ"), й—*послѣ* гласной. Буквы ъ, ь имѣютъ свое мѣсто непремѣнно послѣ согласныхъ и обыкновенно въ концѣ словъ. Самымъ частымъ сочетаніемъ 2-хъ согласныхъ является *ст*. Самымъ частымъ сочетаніемъ двухъ одинаковыхъ буквъ въ серединѣ слова является *нн*. Этимъ мы можемъ закончить нашу экскурсію. Замѣтимъ, что русскій языкъ заключаетъ гораздо менѣе благопріятныхъ для дешифрированія буквенныхъ сочетаній, чѣмъ другіе языки. Напр., въ нѣмецкомъ языкѣ весьма часты комбинаціи ei, ch, ck, sch, th и т. п., во французскомъ—ai, eu, au. eau, eur и т. д. Кромѣ того имъ свойственно употребленіе членовъ, а въ англійскомъ—употребленіе члена the является прямо предательскимъ. Но и приведенныхъ данныхъ совершенно достаточно. Если къ нимъ прибавить знаніе и пониманіе системы да еще наличность извѣстной дозы сообразительности, то получимъ волшебную палочку, противъ которой не устоитъ ни одинъ шифръ (за немногими исключеніями). Разумѣется, текстъ криптограммы долженъ быть настолько великъ, чтобы въ немъ хоть въ слабой степени могли отразиться фонетическіе законы и свойства системы.

Всѣ шифры, о которыхъ говорятся въ настоящей книгѣ, можно классифицировать такъ.

А. Постояннозначныя системы:

I. Единозначныя системы:

1) *Единозначный парный* шифръ (со взаимозамѣщеніемъ буквъ въ парѣ);
2) Единозначный непарный (безъ взаимозамѣщенія).

II. Многозначныя системы:

a) Искусственные шифры:

3) *Простой квадратный;*
4) *Сложный квадратный* (съ однимъ горизонтальнымъ распредѣлителемъ);
5) Сложный квадратный съ нѣсколькими горизонтальными распредѣлителями;
6) Сложный квадратный съ горизонтальными и вертикальными распредѣлителями;
7) Сложный квадратный съ 2 ключами;
8) *Прерывистый квадратный* (съ фиктивными цифрами);
9) Раціональный квадратный.

b) Естественные шифры:

10) Книжный.
11) Стихотворный.

Б. Перемѣннозначныя сисстемы:

I. Непеpіодическія системы:

12) *Множественный квадратный.*

II. Періодическія системы:

13) *Раздѣльный періодическій* (Гамбеттовскій);
14) *Сокращенный Гамбеттовскій;*
15) Замаскированный Гамбеттовскій (Наполеоновскій);
16) Разностный Гамбеттовскій;
17) Слитный періодическій (съ однороднымъ ключемъ);
18) Слитный періодическій (съ разнороднымъ ключемъ);
19) Вторичный періодическій (комбинація съ квадратнымъ).

Постоянно значными системами я называю такія, въ которыхъ каждый знакъ означаетъ *одну* опредѣленную букву (хотя каждая буква можетъ выражаться *нѣсколькими* знаками). Напр., если при данной системѣ и ключѣ *25* означаетъ *б*, то въ любомъ мѣстѣ текста подъ этимъ числомъ скрывается непремѣнно *б*. Въ перемѣнно значныхъ, наоборотъ, какой-нибудь знакъ *25* выражаетъ въ одномъ мѣстѣ *б*, въ другомъ *м*, въ третьемъ *ш* и т. д.

Искусственными системами я называю тѣ, гдѣ ключомъ служитъ условленная фраза, слово, число, при помощи которыхъ составляется искусственно таблица знаковъ или измѣняется текстъ письма. Естественными же я называю тѣ, гдѣ таблица знаковъ имѣется готовою, въ формѣ естественнаго печатнаго или писаннаго скопленія буквъ (напр., печатная страница или стихотвореніе). Курсивомъ отмѣчены наиболѣе употребительные шифры.

Со слѣдующей главы мы приступаемъ къ разбору шифровъ. Въ своемъ изложеніи мы, однако, для удобства нѣсколько отступимъ отъ того порядка, въ которомъ системы приведены въ классификаціонной таблицѣ.

Глава II.

ЕДИНОЗНАЧНЫЙ ПАРНЫЙ ШИФРЪ.

Ты, земледѣлецъ, будь мореходцемъ.
Ты, мореходецъ, станешь сейчасъ земледѣльцемъ.
[Ступайте,
Мѣсто свое помѣнявъ, ты — туда, ты — сюда!
Горацій, Сатиры.

„Но, — сказалъ я, возвращая ему листокъ, — для меня это китайская грамота, я тутъ ничего не разберу, хотя бы мнѣ предложили всѣ алмазы Голконды за разъясненіе этой тарабарщины".

— А между тѣмъ, — возразилъ Легранъ, — разгадать этотъ шифръ вовсе не такъ трудно, какъ это вамъ можетъ показаться съ перваго взгляда...
Эдгаръ Поэ, „Золотой жукъ".

Если записать любой текстъ буквами чужой азбуки, напр., русскую рѣчь арабскими или еврейскими, то она становится для огромнаго большинства совершенно непонятной. Желающему сдѣлать какую-либо запись недоступной для всѣхъ, кромѣ посвященныхъ, легко отсюда придти къ мысли замѣнить буквы алфавита какими-нибудь условными знаками. Таковыми могутъ служить всевозможнѣйшія сочетанія изъ палочекъ, точекъ, кружковъ и т. п. Въ извѣстномъ разсказѣ Эдгара Поэ „Золотой жукъ" мѣстонахожденіе клада зашифровано именно этимъ первобытнымъ способомъ. Англійскія буквы тамъ замѣнены цифрами, знаками препинанія, крестиками. Это типичный случай простого единозначнаго шифра *).

---

*) Къ той же категоріи относится и такъ называемый „Двубуквенный шифръ Бэкона", по поводу котораго одна американская дама, г-жа Галлупъ, выпустила не-

Очевидно, корреспондентамъ приходится запомнить или держать у себя записанными столько условныхъ знаковъ, сколько въ азбукѣ буквъ. Ясно, что для революціонныхъ цѣлей такой шифръ совершенно не годится. Ключъ долженъ быть у корреспондентовъ въ головѣ, а не въ записной тетради, а для этого нужно, чтобы онъ былъ легкимъ для запоминанія. Если даже съ обыкновенными ключами, состоящими изъ одного слова, выходитъ зачастую путаница и недоразумѣнія, то легко представить себѣ, какую кучу ошибокъ надѣлали бы они, еслибъ понадѣялись, что память ихъ удержитъ 34 условныхъ обозначенія, несвязанныхъ между собою никакой нитью. А вѣдь нерѣдко приходится вести сношенія одновременно со множествомъ лицъ при различныхъ ключахъ.

Неудивительно, что чистая форма единозначнаго шифра совершенно не употребительна у насъ. Зато въ большомъ ходу упрощенная модуляція его, которую мы назвали парнымъ единозначнымъ шифромъ.

Представимъ себѣ фразу или сочетаніе словъ, содержащее въ себѣ 17 *различныхъ* буквъ, т. е. половину алфавита. Пусть это будетъ, напр., „желѣзный шпицъ дома". Оставшіяся 17 буквъ подпишемъ подъ этой фразой въ алфавитномъ порядкѣ:

желѣзный шпицъ дома
бвгікрст уфхчщ ьэюя

Каждая верхняя буква съ лежащей подъ ней нижней составляетъ *пару*, въ которой одна взаимно замѣщается другою. Напр., буква *ж* изображается *знакомъ б*; наоборотъ *буква б* обозначается посредствомъ *ж*. Такихъ паръ окажется, слѣдовательно, семнадцать. Фраза: „письмо получено" зашифруется такъ: фхыдюэфэгшщврэ. Нетрудно замѣтить, что знаками служатъ здѣсь тѣ же 34 буквы азбуки, только съ другимъ смысломъ, причемъ каждая буква имѣетъ лишь одно обозначеніе. Слѣдовательно, отличіе его отъ другихъ единозначныхъ системъ заключается въ томъ, что знаками служатъ здѣсь исключительно буквы, что одна половина знаковъ взаимно связана съ другой половиной, и что ключъ весьма удобенъ для запоминанія.

Особенности системы. Для практическаго примѣненія этотъ шифръ весьма удобенъ. Составить табличку отнимаетъ чрезвычайно мало времени; пользованіе ею не представляетъ никакихъ трудностей; зашифрованный текстъ занимаетъ мало мѣста благодаря тому, что буква замѣняется буквой же. Что касается надежности его, то хотя каждая буква обладаетъ лишь однимъ обозначеніемъ, зато отдѣльная пара совершенно независима отъ остальныхъ и распознаваніе одной не даетъ прямыхъ нитей для угадыванія слѣдующихъ.

давно книгу, доказывая, что въ произведеніяхъ Шекспира скрываются важные зашифрованные документы, и что его сочиненія написаны Бэкономъ.

„Представьте себѣ.—говоритъ она,—что два лица, находящіяся между собою въ перепискѣ, уславливаются писать шифромъ, состоящимъ всего изъ двухъ буквъ, но въ извѣстной группировкѣ—по 5 буквъ въ словѣ. Напр.:

A=aaaaa	H=aabbb	P=abbba	X=babab
B=aaaab	J,j=abaaa	Q=abbbb	Y=babba
C=aaaba	K=abaab	R=baaaa	Z=babbb
D=aaabb	L=ababa	S=baaab	
E=aabaa	M=ababb	T=baaba	
F=aabab	N=abbaa	U, V=babaa	
G=aabba	O=abbab	W=bbaaa	

Представимъ себѣ, что въ письмѣ, которымъ обмѣняются пара лицъ, каждая буква представляетъ или **a** или **b** тайной азбуки. Буквы **b** будутъ написаны курсивомъ (кривыми буквами), а прямыя буквы будутъ означать **a**. Получивъ письмо, онъ вмѣсто кривыхъ буквъ ставитъ **b**, а вмѣсто прямыхъ—**a**, и у него получится извѣстное сочетаніе этихъ буквъ, смыслъ которыхъ ему нетрудно будетъ угадать по приведенной азбукѣ".

Несмотря на внѣшній замысловатый характеръ этой системы, сущность ея весьма примитивная. Каждая буква имѣетъ лишь одно обозначеніе, только вмѣсто комбинацій черточекъ и цифръ тутъ служатъ знаками всевозможныя сочетанія изъ двухъ буквенныхъ элементовъ. Разбору простого единозначнаго шифра посвящена слѣдующая глава.

Задача. Требуется расшифровать слѣдующій отрывокъ *):

йрчщзжхшифйэлэчс[3]ямчйщзмъірѣръхшзцгшхсефтйфяорнкзшхмйгэхркреійэрвищ ъхщцгзшхэнсешяйшм[1]ызэгшшъзшяйш[2]хфхсдрзшящнсймпшычэмйркгхэзъ*вк*шъхэямхіке рыеэчфяшзійшнъх *мтъ* мкешхмяшкшзшюйэышцрерыэйрцгзшъшяъшнсяшчэязмяэзэъіяс фзмбгмкрерфэшмъзшцшчгшхсшшхшетнштъхэяэзмъішчйщнегомъзшяйшъэвгрчшнэфозм кшчслризжирючфймнмк*шзлэ*зшчящхемзшчиммъхшвзсхэпшнпемпспэпшнцгяэрхсйэйшд йгтскшюэеэтс.

Распознаваніе системы. Опредѣлить, съ какой системой мы имѣемъ дѣло, не представило бы никакихъ затрудненій. Такой видъ—буквенные знаки, числомъ 34—имѣетъ только парный единозначный шифръ. Смѣшеніе возможно только съ непарнымъ шифромъ, описываемымъ въ слѣдующей главѣ, но и ихъ легко отличить другъ отъ друга, какъ это будетъ тамъ показано.

Раскрытіе шифра. Выпишемъ всѣ встрѣчающіеся въ нашей криптограммѣ знаки, подсчитаемъ, сколько разъ каждый встрѣчается тамъ, и расположимъ ихъ въ убывающемъ порядкѣ. Это основной пріемъ при дешифрированіи, дающій всегда цѣнный базисъ для дальнѣйшаго анализа. При такомъ подсчетѣ, между прочимъ, выступаютъ наружу неизбѣжные грѣхи пишущаго, который почти всегда шифруетъ, какъ богъ на душу положитъ, безъ сознательнаго отношенія къ дѣлу, безъ достаточнаго пониманія, зачастую даже не видя того, что выводитъ его перо. Но это мимоходомъ. Въ данномъ случаѣ никакихъ „грѣховъ" не можетъ быть. Буквы имѣютъ только по одному обозначенію, выбирать не изъ чего, и зашифрованный текстъ можетъ имѣть только *одинъ* видъ.

Для удобства читателей, во избѣжаніе путаницы, мы въ этой, равно и слѣдующей главѣ будемъ обозначать буквы, какъ *знаки*, посредствомъ прописныхъ буквъ, а *значенія* ихъ—посредствомъ малыхъ буквъ. Равенство Ж=б будетъ обозначать, что подъ знакомъ *Ж* скрывается въ дѣйствительности буква *б*.

Сдѣлавши подсчетъ, мы найдемъ, что 350 буквъ текста распредѣляются въ такой пропорціи:

Таблица № 6.

Ш—43	Ъ—16	К—11	Ы—5	Ж—2
Э—26	Я—16	Ф—9	Т—4	Ѣ—1
З—25	С—14	Щ—8	Л—3	Б—1
М—24	П—13	И—8	В—3	Ь—1
Х—20	Е—12	Ц—6	О—3	А—0
Й—19	Ч—12	І—6	Ю—3	У—0
Р—18	Г—11	Н—5	Д—2	—

Относительно истиннаго характера Ш, стоящаго во главѣ таблицы, не можетъ быть никакого сомнѣнія. Это буква *о*: Ш=о; слѣдовательно, по причинѣ взаимности буквъ въ парѣ, О=ш. Выдѣлимъ, затѣмъ, слѣдующія восемь буквъ, явно принадлежащія къ первому разряду. На всякій случай прихватимъ и девятую, такъ какъ разница между числами не очень велика на границѣ этого разряда, а пограничная *в*, какъ мы уже знаемъ, нерѣдко забирается между перворазрядными. Намъ придется, такимъ образомъ, произвести дифференціальный діагнозъ между слѣдующими 9 буквами:

Э—26; З—25; М—24; Х—20; Й—19; Р—18; Ъ—16; Я—16; С—14.**)

Имъ соотвѣтствуютъ, хотя, можетъ быть, и въ другомъ порядкѣ, буквы:

а, и, е, т, н, с, л, ъ, в.

Первымъ дѣломъ надлежитъ отдѣлить гласныя буквы отъ согласныхъ. Кто же намъ поможетъ отличить тѣхъ отъ другихъ? Никто иной, какъ узнанный уже нами „король". Онъ самъ принадлежитъ къ роду гласныхъ и потому въ непосредственномъ сосѣдствѣ съ собой терпитъ только согласныя буквы. Итакъ, намъ остается лишь про-

*) Стоящія надъ нѣкоторыми буквами сверху цифры означаютъ группы буквъ, о которыхъ ниже будетъ рѣчь и на которыя придется ссылаться; то же и объ отмѣченныхъ курсивомъ.

**) Крайнія буквы этого ряда, если перевести ихъ коэффиціенты по отношенію къ 1000 буквъ, дадутъ для Э число 71,5, а для С—40—какъ разъ предѣлы перваго разряда. Для Ш = о выйдетъ 123 на тысячу.

смотрѣть нашу криптограмму и замѣтить себѣ, какія изъ выдѣленныхъ нами девяти буквъ встрѣчаются рядомъ съ Ш и какія нѣтъ. Буквы тогда размѣстятся такъ:

гласныя	согласныя
Э, М, Р, С.	З, Х. Й. Я, Ъ.

Въ числѣ гласныхъ должна была очутиться и та буква, подъ которой скрывается ъ, потому что она тоже избѣгаетъ быть въ сосѣдствѣ съ Ш.

Займемся сперва гласными. Необходимо опредѣлить, какіе изъ четырехъ знаковъ: Э, М, Р, С и четырехъ значеній ихъ: а, е, и, ъ, соотвѣтствуютъ другъ другу. Для этого выпишемъ изъ таблицы 6-ой коэффиціенты послѣднихъ, какъ *знаковъ*, т. е. посмотримъ, какъ часто встрѣчаются въ нашемъ текстѣ знаки А, Е, И, Ъ. Получимъ, такимъ образомъ, два квартета:

Э — 26	А — 0
М — 24	Е — 12
Р — 18	И — 8
С — 14	Ъ — 17

Каждая буква одного квартета имѣетъ себѣ пару въ другомъ. Это въ нѣкоторомъ родѣ экзогамный бракъ. Распознать суженаго нѣтъ ничего легче, если помнить про взаимность буквъ въ парѣ. Э=26; съ перваго же взгляда видно, что Э нарядилась въ павлиньи перья; она сама по себѣ занимаетъ предпослѣднее мѣсто въ алфавитѣ по частотѣ, и по настоящему она должна обладать самымъ ничтожнымъ коэффиціентомъ. Какая же изъ перваго квартета болѣе всего соотвѣтствуетъ по своей числовой величинѣ обиженной природой э? Очевидно А, коэффиціентъ которой — нуль. Итакъ, Э=а, и наоборотъ, А=э.

Изъ остальныхъ трехъ буквъ лѣваго квартета самой частой въ алфавитѣ является *с*; ей должна, поэтому, соотвѣтствовать изъ правой четверки буква съ наибольшимъ коэффиціентомъ, т. е. Ъ. Итакъ С=ъ; Ъ=с.

Остается сбросить маски съ М — 24 и Р — 18, которымъ соотвѣтствуютъ Е — 12, И — 8. Буква Р употребительнѣе, чѣмъ М, поэтому ей должна скорѣе соотвѣтствовать Е, обладающая большимъ числовымъ значеніемъ, чѣмъ ея товарка И. Слѣдовательно, Р=е: Е=р; М=и; И=м.

Перейдемъ къ разсортированію пяти согласныхъ: З, Х, Й, Я, Ъ, подъ которыми скрываются: т, л, н, с, в.

Относительно Ъ мы уже узнали, что онъ обозначаетъ *с*. Если бы мы захотѣли поступить по прежнему методу и сопоставили два новыхъ квартета:

З — 25	Л — 3
Х — 20	В — 3
Й — 19	Т — 4
Я — 16	Н — 5,

то сейчасъ бы увидѣли, что имъ тутъ нельзя воспользоваться: коэффиціенты праваго квартета слишкомъ мало отличаются другъ отъ друга, чтобы служить надежнымъ путеводителемъ. Поэтому прибѣгнемъ къ другому методу — „исключенія". Присматриваясь къ тексту, мы найдемъ въ немъ слѣдующія отмѣченныя курсивомъ сочетанія буквъ: 1) ъвк, 2) мть, 3) шзл.

Въ первомъ сочетаніи ЪВК знакъ В стоитъ послѣ Ъ, т. е. послѣ *с*, слѣдовательно, никакъ невозможно, чтобы подъ буквой В скрывалась *й*, ибо послѣдняя стоитъ всегда только послѣ гласныхъ.

Во второмъ сочетаніи МТЬ знакъ Т стоитъ послѣ М, т. е. послѣ *и*. Слѣдовательно, и Т не можетъ обозначать *й*, ибо послѣдней никогда не предшествуетъ *и*, а всегда і.

Въ третьемъ сочетаніи ШЗЛ — Л стоитъ послѣ З; но подъ З, какъ мы знаемъ, скрывается согласная, слѣдовательно и Л не можетъ соотвѣтствовать *й*.

Если, такимъ образомъ, стоящая въ лѣвомъ квартетѣ Й не состоитъ въ парѣ ни съ *л*, ни съ *в*, ни съ *т*, то ясно, что единственно возможная комбинація — это Й=я; Н=й.

Выпишемъ теперь изъ текста сочетаніе буквъ, находящееся недалеко отъ начала и отмѣченное цифрой [1]: стяйшм; оно стоитъ послѣ С, т. е. послѣ ъ, а потому, вѣроятно, представляетъ начало слова; подставляя извѣстныя уже намъ значенія буквъ, получимъ: ..ро(Я)ноп... Угадать это слово нетрудно даже и безъ добавочныхъ свѣдѣній, но мы къ тому вѣдь знаемъ, что подъ Я можетъ скрываться лишь одна

изъ трехъ буквъ: л, в, т. Ясно, что прочесть его надо: *ровно и*. Слѣдовательно, Я=в; В=я.

Вторая группа буквъ ([2]): ..шъзшяйш..., послѣ подстановки, дастъ: ...ос(З)овно... Выбирать для З приходится только между *л, т*. Разумѣется, читать надо: *словно*; З=л; Л=з. Отсюда также неизбѣжно слѣдуетъ, что послѣдняя изъ перворазрядныхъ согласныхъ *т* выражается посредствомъ Х : Х=т.

Теперь раскрытіе текста пойдетъ уже такъ легко, какъ будто весь ключъ былъ уже въ нашихъ рукахъ. Возьмемъ группу буквъ у самаго начала ([3]): хшифйэлэчс. Подставивъ извѣстныя значенія, имѣемъ: том(Ф)наза(Ч)ъ. Ясно, что это — *тому назадъ*. Ф=у; Ч=д и обратно. Непосредственно предшествующія начальныя 6 буквъ: йрчщзж=нед. л.=недѣлю; Щ=ѣ. Послѣдующая же группа: ямчйщзмъі=виднѣлис. =виднѣлись. Повторяемъ, чтеніе криптограммы будетъ происходить совершенно безпрепятственно. Вотъ ея содержаніе:

„Недѣлю тому назадъ виднѣлись еще столбы отъ рухнувшей плотины, а теперь на ея мѣстѣ было такъ ровно и гладко, словно тутъ человѣкъ никогда и не пытался поставить преграду вольной стихіи; противоположнаго берега не было совсѣмъ; вода вливалась въ улицы и переулки слободы, отъ которой оставались однѣ крыши, словно самые дома ушли подъ землю; между ними ползало двѣ-три лодки и стоялъ такой крикъ, какой бываетъ на ночныхъ пожарахъ".

Истинныя значенія всѣхъ буквъ текста видны изъ слѣдующей таблички:

а=э	г=ы	ж=ю	і=ь	о=ш	у=ф
б=ц	д=ч	з=л	й=н	с=ъ	щ=ѣ
в=я	е=р	и=м	к=п	т=х	

Задача рѣшена, шифръ разобранъ. Единственное, чего не хватаетъ для увѣнчанія зданія — это знаніе ключа въ его естественномъ, мнемоническомъ видѣ, т. е. той фразы изъ 17 буквъ, которая даетъ найденныя нами значенія буквъ. Для спеціальнаго бюро Департамента Полиціи это, разумѣется, совершенно излишне; товарищамъ же приходилось разрѣшать на практикѣ и этотъ вопросъ. Когда ошибка корреспондента, спутавшаго ключъ, вынуждала браться за расшифрованіе безъ ключа, то, когда дѣло шло о единозначномъ парномъ шифрѣ, приходилось добираться и до ключа, чтобы легче его запомнить. Несмотря на то, что на первый взглядъ задача кажется совсѣмъ неразрѣшимой, ибо 17 паръ допускаютъ билліоны перестановокъ, однако, въ дѣйствительности, дѣло совсѣмъ легкое *).

Взятый нами для анализа зашифрованный текстъ заключаетъ, какъ мы видѣли,

---

*) Вспомнимъ, какъ составляется ключъ. Наверху пишется условная фраза, т. е. два-три слова съ живымъ, благозвучнымъ сочетаніемъ буквъ; внизу *въ алфавитномъ порядкѣ* остальныя 17 буквъ, въ большинствѣ *мало* употребительныя. Возьмемъ первую найденную пару а=э; въ ключѣ обѣ буквы пишутся одна *надъ* другой. Какое же положеніе вѣроятнѣе: $\frac{а}{э}$ или $\frac{э}{а}$? Если примемъ во вниманіе, что, съ одной стороны, *э* почти самая рѣдкая буква, а съ другой стороны — безъ *а* весьма трудно составить фразу изъ 17 различныхъ буквъ, для которой приходится мобилизировать большинство гласныхъ, то, конечно, предпочтемъ $\frac{а}{э}$; но въ такомъ случаѣ эта парочка помѣщается обязательно на правомъ флангѣ ключа, ибо *э* занимаетъ вѣдь одно изъ послѣднихъ мѣстъ въ азбукѣ, а внизу буквы идутъ въ алфавитномъ порядкѣ. Буквѣ *э* непосредственно предшествуетъ *щ*, сопряженная съ *ш*. Вопросъ только въ томъ, подходитъ ли пара $\frac{щ}{ѣ}$ къ прежней $\frac{а}{э}$; иными словами, получится ли наверху благозвучное сочетаніе. Относительно *ша* вопросъ рѣшается утвердительно. Передъ *щ* стоитъ въ азбукѣ *ъ*, спаренная съ *і*; но сочетаніе *іша* совсѣмъ невозможно; слѣдовательно, изъ двухъ положеній $\frac{і}{ъ}$ и $\frac{ъ}{і}$ надо выбрать вторую; но она стоитъ въ ключѣ, конечно, гораздо ближе къ лѣвому флангу, ибо *і* одна изъ начальныхъ буквъ. Буквѣ *ъ* предшествуетъ *ы*, находящееся въ одной парѣ съ *г*, но и *гша* никуда не годится; поэтому предпочитаемъ $\frac{ы}{г}$, которую приходится отодвинуть еще болѣе влѣво. Передъ *ы* стоитъ въ азбукѣ *ъ*=*с*. Сочетаніе *сша*, однако, тоже нельзя

350 буквъ. Разборъ шелъ совершенно безпрепятственно, какъ будто чтеніе со словаремъ въ рукѣ. Если бы текстъ былъ значительно короче, напр., изъ 100—50 буквъ, то фонетическіе законы были бы выражены въ немъ несравненно менѣе отчетливо. Дѣло разгадки шло бы не съ такой ровностью и увѣренностью, неоднократно попадали бы на ложный путь, но конечный результатъ былъ бы тотъ же.

Заключеніе. Ясно, что разобранную систему никоимъ образомъ нельзя рекомендовать; ея безусловно не слѣдуетъ примѣнять. Только для временныхъ краткихъ записей она можетъ еще быть пригодной, да и то съ извѣстными оговорками (см. гл. XXI). Съ другой стороны, она допускаетъ нѣкоторыя раціональныя улучшенія, благодаря которымъ она, впрочемъ, теряетъ совершенно характеръ единозначности (см. гл. XIX).

Глава III.

НЕПАРНЫЙ ЕДИНОЗНАЧНЫЙ ШИФРЪ.

Ты, мишенька, садись противъ альта,
Я, прима, сяду противъ вторы;
Тогда пойдетъ ужъ музыка не та,
У насъ запляшутъ лѣсъ и горы.

Крыловъ.

Разобранный нами шифръ отличается отъ чистыхъ формъ единозначнаго шифра главнымъ образомъ тѣмъ, что половина буквъ связана съ другой половиной. Это обстоятельство, конечно, облегчаетъ разгадку. Исходя, однако, изъ его принципа, можно легко построить шифръ, который, будучи столь же легкимъ для запоминанія и почти столь же удобнымъ, въ то же время уничтожилъ бы всякую зависимость между знаками. Для этого нужно лишь взять двойной ключъ.

Воспользуемся уже знакомыми намъ двумя 17-ти буквенными фразами: 1) желѣзный шпицъ дома и 2) цырюльникъ худощавъ. Дополнимъ каждую недостающими 17 буквами, но напишемъ ихъ рядомъ съ соотвѣтствующей фразой: въ первой *справа* отъ нея, во второй *слѣва*. Наконецъ, одинъ рядъ (изъ 34 буквъ) подпишемъ подъ другимъ:

желѣзный шпицъ дома бвгікрстуфхчшьэюя
я эѣшчфтс пмйіз жегб цырюльникъ худощав

Это и будетъ ключъ. Каждый горизонтальный рядъ заключаетъ въ себѣ полную азбуку. Каждая буква нижняго ряда служитъ знакомъ для соотвѣтствующей верхней буквы. Можно условиться и наоборотъ, т. е. чтобы верхнія служили знаками для нижнихъ; но одновременнаго взаимозамѣщенія тутъ уже нѣтъ. Напр., буква *ж* изображается посредствомъ Я, но *я* уже не обозначается обратно посредствомъ Ж, а, какъ видно изъ таблички, посредствомъ В. Тутъ не исключается возможность случайнаго совпаденія буквъ обоихъ рядовъ, благодаря чему какая-нибудь буква выражается посредствомъ себя же. Напр., въ нашемъ примѣрѣ это случилось съ *х*. Ни-

---

назвать удачнымъ; беремъ поэтому $\frac{ъ}{с}$, которая помѣстится приблизительно въ серединѣ ключа. Изъ двухъ буквъ *ш*, *щ*—непосредственно предшествующихъ въ азбукѣ ъ, первая у насъ уже имѣется, а вторая, сопряженная съ *о*, даетъ наверху удовлетворительное соединеніе *оща*. Мы набрали уже довольно значительную часть ключа, которая наглядно представится такъ:

...ы...ь....ъ.... о ща..
....г...і....с....ш ѣ э...

На этомъ мы остановимся, чтобы не удлинять изложенія. Дальнѣйшее возстановленіе ключа пойдетъ такъ же гладко. Въ результатѣ окажется:

ц ы р ю л ь н и к ъ х у д о щ а в.
б г е ж з і й м п с т ф ч ш ѣ э я.

чего дурного въ этомъ нѣтъ. Но можно и этого избѣгнуть, если условиться въ случаѣ совпаденія переставить совпавшую букву на мѣсто сосѣдней.

Такъ какъ изобрѣтать словосочетанія изъ 17 буквъ—задача довольно трудная, то можно упростить дѣло, взявши напр., два любыхъ стиха или двустишія: въ нихъ выкидываются повторяющіяся буквы, пока не наберется 17 разнородныхъ. Въ остальномъ съ ними поступаютъ по вышеописанному.

Возьмемъ, напр., четверостишіе:

1) *Выхожу* *один*ъ *я* на *дорогу*, *сквозь* туманъ....

2) *Ночь тиха*, *пустыня внемлет*ъ Богу....

Выпишемъ отмѣченныя курсивомъ первыя 17 разнородныхъ буквъ изъ каждаго двустишія:

1) выхожудинъяаргскз.

2) ночьтихапусывемл.

Это и будетъ ключъ, замѣняющій двѣ условныя фразы.

Особенности системы. По сравненію съ парнымъ разбираемый здѣсь шифръ теряетъ нѣсколько въ смыслѣ удобства примѣненія, такъ какъ составленіе таблички отнимаетъ больше времени. За то раскрыть его труднѣе, ибо между знаками нѣтъ и тѣни искусственной зависимости. Этимъ онъ отличается въ благопріятную сторону рѣшительно отъ всѣхъ искусственныхъ, въ которыхъ между знаками существуютъ всегда болѣе или менѣе сложныя и явныя взаимоотношенія. Это—система, въ которой при разборѣ знаніе внутренней структуры ключа не даетъ ничего, а дешифрированіе основано исключительно на знаніи фонетическихъ законовъ и догадливости.

Задача. Въ нижеслѣдующей криптограммѣ мы нарочно выбросили букву ъ, потому что она почти всегда выпускается, а между тѣмъ употребленіе ея даетъ, послѣ того какъ она узнана, извѣстный плюсъ отгадчику: она помогаетъ отдѣлять слова другъ отъ друга.

Бэриджлтпгэлхтъщэдыіщжеьжйгтетитеэъюфтъпцц[2]іеэггвтдю[4]офюъэеюпипмфтъэгэъц[1]лъщтфтдюотхзжеютълчщэгэ,[3]ъщчдюдилэзжлпвбълчщжльфтзтгридвишчгжхтъщггчщвб[5]отхзжеюажщлтфэгэажтмтнзлифцьжйдыглъщифэажпилигэгшыежыъщтьжеэгиржлиыілыхгжй.

Распознаваніе системы. Что передъ нами единозначный шифръ, это видно съ перваго взгляда. Остается лишь отличить его отъ парнаго. Это становится возможнымъ послѣ подсчета знаковъ:

Таблица № 7.

Т—21	Щ—12	Ы—6	Х—4	Б—3	У—0
Э—16	И—10	Ч—6	Ь—4	Ц—2	Я—0
Ж—16	Ф— 8	П—5	А—3	Н—2	Ѣ—0
Г—15	Д— 8	В—4	І—3	О—2	С—0
Л—14	Ю— 8	З—4	М—3	Ш—1	
Ъ—13	Е— 8	Й—4	Р—3	К—0	

Очевидно, что Т, какъ самый частый знакъ, служитъ маской для *о*. Если мы имѣемъ передъ собой парный шифръ, то, вслѣдствіе взаимности, О=т. Но *т* перворазрядная согласная; она встрѣчается въ языкѣ часто, слѣдовательно, ея знакъ О долженъ и въ нашемъ текстѣ обладать большимъ коэффиціентомъ. Въ дѣйствительности же она попадается всего два раза. Ясно, что въ данномъ случаѣ система непарная.

Раскрытіе шифра. Послѣ того, какъ сдѣланъ подсчетъ 208 буквъ криптограммы и разыскана буква *о*, намъ надо заняться первымъ разрядомъ. За вычетомъ отсутствующаго твердаго знака, отбираемъ 7 высшихъ буквъ: Э, Ж, Г, Л, Ъ, Щ. И. По настоящему слѣдовало бы захватить еще одну, для пограничной, но бѣда въ томъ, что далѣе слѣдуютъ цѣлыхъ 4 буквы съ однимъ и тѣмъ же коэффиціентомъ 8. Какую именно изъ нихъ присоединить къ тѣмъ, мы не знаемъ, и потому лучше ограничимся нашими семью, но будемъ помнить, что среди нихъ могла затесаться буква *в*, которая, конечно, вытѣснила внизъ какую-нибудь перворазрядную.

Съ помощью любезнаго руководителя Т=о мы и тутъ живо отдѣлимъ гласныя отъ согласныхъ.

гласныя:	согласныя:
Э, Ж, И.	Г, Л, Ъ, Щ.

Внимательно просматривая текстъ, мы замѣчаемъ, что въ такомъ маленькомъ отрывкѣ комбинація двухъ перворазрядныхъ согласныхъ ЪЩ встрѣчается цѣлыхъ шесть разъ. Иными словами, половина всѣхъ экземпляровъ Ъ и Щ заключена въ этой комбинаціи. Нетрудно догадаться, что это *ст*, такъ какъ только это сочетаніе согласныхъ встрѣчается въ такой высокой пропорціи *). Итакъ Ъ=с; Щ=т. Подъ остальными двумя согласными скрываются л, н, либо в.

Выберемъ группу буквъ (1):... мфтъэгэъц... Въ ней намъ вполнѣ достовѣрно извѣстны только Т. Ъ. Подъ Э можетъ скрываться *а*, *е* или *и*; подъ Г—*л*, *н* или *в*. Ф, судя по коэффиціенту (8)—второразрядная согласная: р, п, к.. Подставляя, мы получаемъ такое неопредѣленное выраженіе:

а л а
...о с е н е с.
и в и

Изъ разнообразныхъ возможныхъ сочетаній остановиться стоитъ только на ...*осалась* или ..*осились*. Во всякомъ случаѣ Г=л; Ц=ь: Э=$^{а}_{и}$. Глаголъ же, которому принадлежитъ этотъ обрывокъ, можетъ быть одинъ изъ такихъ: просились, бросились, бросалась, носились, косились. Слѣдовательно, Ф либо *н*, либо *р*. Но сейчасъ за этимъ слѣдуетъ: лщтфтдю.., причемъ Д тоже обладаетъ высокимъ коэффиціентомъ. Такъ какъ за Л остается только значеніе *в*, то намъ приходится выбирать между:

$^{п}_{б}$росились въ сторо..
носились въ стоно..

Первая комбинація естественнѣе, тутъ можно предполагать *в сторону(ы)*. Слѣдовательно, Ф=р; Д=н; Ю=*у* или *ы*. Послѣднее сомнѣніе, впрочемъ, сейчасъ же разрѣшается изъ группы (2): ъюфтъщц=с$^{ы}_{у}$рость=сырость. Слѣдовательно Ю=ы.

Остающійся все еще сомнительнымъ вопросъ, что скрывается подъ Э—*а* или *и*, рѣшается изъ группы (3): тълчщэгэ=осв. т$^{и}_{а}$л$^{и}_{а}$=освѣтили. Значитъ, Ч=ѣ; Э=и. Сейчасъ за этимъ словомъ слѣдуетъ: ъщчдю=стѣны.

Группа (4): еэггвтдю=. илл. оны=милліоны; Е=м. Группа (5): шчгжхтъщтгчщвб=. ѣл$^{а}_{е}$. остолѣті. =цѣлаго столѣтія. Ш=ц; Ж=а (значитъ послѣдняя перворазрядная гласная И=е); Б=я.

Дальше продолжать углубляться не стоитъ; никакихъ затрудненій встрѣтиться уже не можетъ. Истинный характеръ знаковъ изобразится въ такой табличкѣ:

Таблица № 8.

А=з	Ж=а	Л=в	(С=ъ)	Ч=ѣ	(Ѣ=э)
Б=я	З=д	М=б	Т=о	Ш=ц	Э=и
В=і	И=е	Н=й	(У=ф)	Щ=т	Ю=ы
Г=л	І=ю	О=к	Ф=р	Ъ=с	Я=ч
Д=н	Й=х	П=ш	Х=г	Ы=у	
Е=м	(К=щ)	Р=ж	Ц=ь	Ь=п	

Раскрытый текстъ гласитъ: „Я и жена вошли въ гостиную. Тамъ пахло мохомъ и сыростью. Милліоны крысъ и мышей бросились въ стороны, когда мы освѣ-

*) На 1000 буквъ оно попадается 15-30 разъ. Другія, не менѣе благозвучныя сочетанія, какъ, напр., *сл*, *св*, встрѣчаются несравненно рѣже. Вотъ нѣкоторыя причины такого значительнаго преобладанія этой пары. Корень *ст* общъ всѣмъ древнимъ и новымъ языкамъ и у насъ входитъ въ составъ множества русскихъ и иностранныхъ словъ; помимо того это сочетаніе входитъ въ составъ нѣсколькихъ другихъ корней. Затѣмъ оно участвуетъ во множествѣ суффиксовъ простыхъ и сложныхъ: ство, ость, истъ, астъ, истика и т. д. Наконецъ, нѣкоторыя буквы, напр., з, т, д, передъ *т* переходятъ въ *с*. Примѣры: *достоинство*, *статистъ*, *растрата*, *страстность*. Въ криптограммѣ предыдущей главы оно встрѣчается тоже 6 разъ. Впрочемъ, незачѣмъ далеко ходить: въ настоящемъ примѣчаніи, за вычетомъ примѣровъ, его имѣется 11 штукъ! Это воистину предательская пара.

тили стѣны, не видавшія свѣта въ продолженіе цѣлаго столѣтія. Когда мы затворили за собою дверь, пахнулъ вѣтеръ и зашевелилъ бумагу, стопами лежавшую въ углахъ".

Ключемъ послужило здѣсь четверостишіе:

1) И пусть у гробового входа
Младая будетъ жизнь играть
2) И равнодушная природа
Красою вѣчною сіять.

Буквы, заключенныя на таблицѣ № 8 въ скобки, вовсе не встрѣчаются въ текстѣ задачи.

Заключеніе. Этотъ шифръ нѣсколько труднѣе для разгадки, чѣмъ предыдущій; но, тѣмъ не менѣе, приговоръ надъ нимъ не можетъ быть иной: его никоимъ образомъ нельзя рекомендовать.

Глава IV.

ПРОСТОЙ КВАДРАТНЫЙ ШИФРЪ.

„Постойте, я сыскалъ секретъ!"-
—Кричитъ оселъ: Ужъ вѣрно мы поладимъ,
Коль рядомъ сядемъ".
Послушались осла, усѣлись чинно въ рядъ..
Крыловъ.

Предыдущей главой мы покончили съ буквенными системами и отнынѣ до конца книги мы будемъ имѣть дѣло только съ такими, гдѣ знаками служатъ *числа*. Царство чиселъ велико и обильно, и порядокъ въ немъ ввести нетрудно. Самый естественный способъ завести стройный порядокъ заключается въ томъ, чтобы расположить условнымъ путемъ скомбинированныя буквы въ нѣсколько горизонтальныхъ рядовъ, въ формѣ квадрата или прямоугольника, и затѣмъ пронумеровать горизонтальные ряды и вертикальные столбцы. Тогда каждая буква изобразится двумя числами, изъ которыхъ одно покажетъ, въ какомъ ряду находится буква, а другая—, какое мѣсто въ этомъ ряду она занимаетъ. Таковъ основной принципъ квадратнаго шифра, который въ нѣсколькихъ модуляціяхъ безспорно представляетъ употребительнѣйшую у насъ систему.

Пусть будетъ у насъ ключомъ десятибуквенная фраза или часть ея: „эта коробка". Начертимъ квадратъ, раздѣлимъ его прямыми линіями на 10 вертикальныхъ и 10 горизонтальныхъ рядовъ, т. е. на 100 квадратиковъ. Въ первомъ лѣвомъ вертикальномъ столбцѣ размѣстимъ нашъ ключъ (Таблица № 9) и, начиная съ буквы ключа, заполнимъ каждый горизонтальный рядъ въ алфавитномъ порядкѣ. Послѣ этого пронумеруемъ сверху и слѣва вертикальные и горизонтальные ряды. Это и составитъ необходимую табличку — магазинъ знаковъ. При шифрованіи обыкновенно раньше пишутъ цифру горизонтальнаго ряда, а потомъ вертикальнаго столбца, но можно и наоборотъ. Для *а* мы найдемъ въ этой таблицѣ 3 знака: 14, 31, 01.

Таблица № 9.

	1	2	3	4	5	6	7	8	9	0
1	э	ю	я	а	б	в	г	д	е	ж
2	*т*	у	ф	х	ц	ч	ш	щ	ъ	ы
3	*а*	б	в	г	д	е	ж	з	и	і
4	к	л	м	н	о	п	р	с	т	у
5	*о*	п	р	с	т	у	ф	х	ц	ч
6	*р*	с	т	у	ф	х	ц	ч	ш	щ
7	*о*	п	р	с	т	у	ф	х	ц	ч
8	*б*	в	г	д	е	ж	з	и	і	й
9	к	л	м	н	о	п	р	с	т	у
0	*а*	б	в	г	д	е	ж	з	и	і

Фраза „письмо получено" можетъ быть выражена по этой таблицѣ такъ: 46, 39, 98, 43, 71, 72, 51, 92, 22, 50, 19, 94, 45. Цифра 0 замѣняетъ десять. Въ данномъ случаѣ, т. е. когда число столбцовъ не превышаетъ десяти, нѣтъ никакой необходимости писать числа раздѣльно; гораздо удобнѣе для пишущаго

писать сплошь, а получателю это не можетъ причинить затрудненій, потому что всѣ числа двузначныя. Иное дѣло, когда число столбцовъ превышаетъ 10. Во-первыхъ, самый ключъ можетъ состоять изъ 15, 20 и даже 30 буквъ. Во-вторыхъ, горизонтальные ряды можно продолжать сколько угодно вправо. Нѣкоторые не лѣнятся даже захватить третью азбуку, заходя за 40. Въ этихъ случаяхъ знакомъ какой-нибудь буквы можетъ служить пара двузначныхъ или однозначныхъ чиселъ или сочетаніе того и другого. Разумѣется, тутъ уже нельзя писать цифры сплошь. Ихъ записываютъ въ формѣ дроби, напр., $^{13}/_{15}$, $^{2}/_{3}$, $^{4}/_{12}$, $^{9}/_{10}$, $^{18}/_{2}$ и т. д. Можно, конечно, и въ этомъ случаѣ придумать способъ для сплошного записыванія; напр., передъ однозначными числами писать нуль. Только что приведенныя для примѣра пять дробей преобразятся такимъ образомъ: 1315020341209101802. При чтеніи письма придется тогда дѣлить числовой рядъ на грани изъ четырехъ цифръ. Можно записывать и короче: вмѣсто 15 писать пять со значкомъ, напр., 5′ или 5,. Тѣ же 5 дробей въ этомъ случаѣ изобразятся совсѣмъ просто: 3′5′2342′90′8′2.

Такова суть простого квадратнаго шифра, который чрезвычайно распространенъ среди нашихъ революціонеровъ.

Особенности системы. Здѣсь ясно видна цѣль — парализовать зловредную фонетическую закономѣрность, которая является столь предательской для шифровъ. Число знаковъ для буквъ, во-первыхъ, сильно увеличено. Во взятомъ нами примѣрѣ, который хотя есть типичный, но содержитъ почти минимальное при данной системѣ число знаковъ, ихъ содержится 100, т. е. почти тройная азбука. Во вторыхъ, соотношенія между буквами въ значительной степени извращены, такъ какъ количество знаковъ для различныхъ буквъ разное. Если ключъ выбранъ умѣло, то неодинаковость знаковъ должна быть цѣлесообразной, т. е. болѣе частыя буквы должны имѣть бо́льшее число комбинацій. Въ нашемъ примѣрѣ о, е встрѣчаются 4 раза, с — 5 разъ, т — 6, а, и — 3 раза, й, ъ, ы, э, ю, я — всего по 1 разу, ь, ѣ вовсе отсутствуютъ. Если бы дешифрированіе опиралось здѣсь, подобно предыдущей системѣ, исключительно на фонетическихъ законахъ, то оно имѣло бы весьма мало шансовъ на успѣхъ. Что касается примѣненія, то этотъ шифръ надо признать весьма удобнымъ: ключъ легко запомнить и сообщить, никакихъ сложныхъ условностей здѣсь нѣтъ, табличку составить отнимаетъ весьма мало времени, а пользоваться ею не представляетъ никакихъ затрудненій. Разумѣется, чѣмъ больше квадратиковъ въ таблицѣ, тѣмъ больше времени отнимаетъ ея составленіе.

Задача. 2302155484416578292459566653499172920865573756628521817752265 3
0332215141576175859543949558666568349804561283524492372633468629119058664912 9
4017166237546694521158497355175650001998883582693877283250885295416917760417 1
2612278125417187887380493246513481594726532931462495278100726954114668814562 5
1129861230122264885646094548634558054157697217157764304.

Распознаваніе системы. Передъ нами сплошной рядъ цифръ, *четный*; по раздѣленіи на грани изъ двухъ цифръ въ каждой, получаемъ рядъ двузначныхъ чиселъ отъ 00 до 99 (правильнѣе было бы сказать: отъ 11 до 00). Это сейчасъ же наводитъ на мысль, что мы имѣемъ дѣло съ квадратнымъ шифромъ. Ясно также, что таблица его имѣетъ 10 × 10 клѣтокъ. Остается лишь узнать, съ какой модуляціей квадратнаго шифра мы тутъ встрѣтились. Это узнается послѣ подсчета знаковъ, и такой сравнительный діагнозъ мы будемъ производить въ слѣдующихъ главахъ, по мѣрѣ знакомства съ варіаціями квадратнаго. Во всякомъ случаѣ, прежде всего слѣдуетъ предположить простой квадратный. Въ случаѣ, если бы таблица превосходила 10×10 клѣтокъ, видъ криптограммы былъ бы иной. Если бы знаки были въ видѣ дробей, то возможно было бы смѣшеніе съ книжнымъ ключомъ (см. глав. XV). Если же числители и знаменатели писать рядомъ безъ перерывовъ со вставками нулей передъ однозначными, то возможно было бы на поверхностный взглядъ смѣшать съ одной формой записыванія гамбеттовскаго шифра (см. гл. VIII и IX).

Раскрытіе шифра. Прежде всего надо сдѣлать обычный подсчетъ знаковъ. Результаты его лучше всего представить на табличкѣ, вполнѣ аналогичной предполагаемой квадратной изъ 10×10 знаковъ. Только вмѣсто неизвѣстныхъ намъ буквъ, въ клѣткахъ разставимъ числа, показывающія, сколько разъ соотвѣтственный знакъ встрѣчается въ текстѣ (табл. № 10). Изъ таблички (задачи), напр., видно, что знакъ *15* встрѣчается 5 разъ, а *60* — два раза.

Припомнимъ, что при этой системѣ буквы въ горизонтальныхъ рядахъ идутъ въ алфавитномъ порядкѣ, а съ другой стороны, что азбука, какъ мы видѣли въ 1-ой

главѣ, распадается на три совершенно различных отдѣла: перворазрядныхъ гласныхъ, центральный и рѣдкихъ буквъ. Ясно, что какъ ни затушевывается при квадратномъ шифрѣ фонетическій законъ, онъ долженъ все же пробиться на таблицѣ, гдѣ нанесены систематическіе коэффиціенты знаковъ. И дѣйствительно, обращая вниманіе на 5-ый горизонтальный рядъ, отличающійся наибольшей полнотой, мы сразу приходимъ къ убѣжденію, что по внѣшнему своему виду, по сравнительно большимъ своимъ коэффиціентамъ, а, главное, по непрерывности этого ряда, онъ принадлежитъ къ центральному отдѣлу, сгруппированному вокругъ буквы *о*. Остается лишь детально опредѣлить отдѣльныя буквы этого ряда, для чего совершенно достаточно узнать хотя бы одну букву. Службу эту можетъ сослужить, напр., знакъ *50*, стоящій въ концѣ нашего ряда. То, что безпрерывный рядъ довольно частыхъ буквъ *) обрывается на этомъ знакѣ, заставляетъ думать, что на мѣстѣ *50* должна была бы стоять *ф*, которая предшествуетъ, слѣдовательно, девятибуквенный рядъ: л, м, н, о, п, р, с, т, у. Вполнѣ правдоподобное предположеніе это можетъ быть немедленно провѣрено и превращено въ полнѣйшую достовѣрность. Стоитъ только сравнить подъемы и спуски нашего ряда на таблицѣ съ подъемами и спусками соотвѣтствующей части кривой на таблицѣ № 5 (I гл.). На таблицѣ № 10, въ пятомъ ряду, пониженія падаютъ на *м*, *п*, *у*, подъемы на л, н, о, р, с, т, что какъ разъ соотвѣтствуетъ взаимному отношенію этихъ буквъ. Итакъ, мы съ увѣренностью можемъ сказать, что знаемъ сразу 10 знаковъ.

Таблица № 10.

	1	2	3	4	5	6	7	8	9	0
1	3	4	—	—	3	—	—	—	—	—
2	4	1	3	2	2	6	2	—	4	—
3	2	2	1	3	1	—	—	—	—	—
4	4	—	2	1	1	5	1	1	3	—
5	4	2	3	4	1	3	3	3	2	—
6	2	2	—	1	4	3	—	2	1	2
7	4	3	1	—	3	2	2	1	—	—
8	4	—	2	2	4	2	2	2	—	2
9	2	2	1	3	3	—	2	2	1	1
0	3	1	1	2	—	—	—	3	—	2

Такимъ же методомъ мы можемъ разгадать еще нѣсколько рядовъ. Прежде всего мы, вообще, замѣчаемъ себѣ, что въ крайнемъ лѣвомъ вертикальномъ столбцѣ заключается *ключъ*, т. е. связное буквенное сочетаніе изъ 10 буквъ. Оно, конечно, не можетъ обходиться безъ гласныхъ, особенно перворазрядныхъ. Пятая буква этого ключа, какъ мы нашли, есть *л*. Мы можемъ допустить, что предшествующая ей буква будетъ гласная. И вотъ, присматриваясь къ 4-му горизонтальному ряду, мы замѣчаемъ сильные подъемы на 1-ой, 6-ой, 9 ой буквахъ, а также небольшое повышеніе на 3 ьей. Одинъ лишь взглядъ на таблицу № 5, гдѣ вверху отчеркнуты „ряды" крупныхъ гласныхъ, покажетъ намъ, что онъ вполнѣ соотвѣтствуетъ десятибуквенному ряду, начинающемуся съ *а*. Подъемы соотвѣтствуютъ какъ разъ *а*, *е*, *и*, также *в*. Десятая нулевая клѣтка отвѣчаетъ буквѣ *і* и т. д. Итакъ, мы имѣемъ еще 10 знаковъ.

Далѣе, при сколько-нибудь внимательномъ изученіи таблицы № 10, нетрудно замѣтить сильную аналогію между узнаннымъ нами уже 4-мъ рядомъ и неизвѣстнымъ еще 2-мъ: тѣ же подъемы на 1-й, 3-й, 6-й, 9-й клѣткахъ; то же паденіе до нуля на 10-ой. Выводъ можетъ быть только такой, что и 2 ой рядъ содержитъ въ себѣ буквы отъ *а* по *і*. Нанесемъ добытые нами результаты для наглядности и облегченія дальнѣйшей работы на таблицу, изображающую обычнаго типа стоклѣточный квадратъ. (Таблица № 11).

Таблица № 11.

	1	2	3	4	5	6	7	8	9	0
1										
2	а	б	в	г	д	е	ж	з	и	і
3										
4	а	б	в	г	д	е	ж	з	и	і
5	л	м	н	о	п	р	с	т	у	ф
6										
7										
8										
9										
0										

Имѣя передъ собою уже раскрытыми цѣлыхъ три ряда (изъ десяти), мы можемъ непосредственно обратиться для дальнѣйшихъ пріобрѣтеній къ тексту. Даже угадавъ одинъ рядъ, можно считать задачу рѣшенной; съ другой стороны, мы могли бы столь же успѣшно продолжать опредѣленіе рядовъ по табл. № 10.

*) Коэффиціенты здѣсь вообще небольшіе, потому что всего-то буквъ въ „задачѣ"

Высмотримъ себѣ въ текстѣ (задачѣ) какое-либо мѣстечко, гдѣ числа изъ извѣстныхъ уже намъ трехъ рядовъ находятся по близости другъ отъ друга въ возможно преобладающемъ количествѣ. Такую группу мы, напр., находимъ недалеко отъ начала:

7752265303322151415761.

Подставляя извѣстныя нами значенія, находимъ:

. мен . . алась . . Не много надо размышлять, чтобы догадаться, что здѣсь скрывается слово: *уменьшалась*, слѣдовательно, 77=у; 03=ь; 32=ш; 61=ь. Значитъ, однимъ ударомъ мы пріобрѣли новыхъ 4 ряда, т. е. новыхъ 40 знаковъ! Теперь мы можемъ уже смѣло взяться за текстъ съ самаго начала и подвигаться совершенно безпрепятственно. Мы въ состояніи, впрочемъ, рѣшить задачу, не заглядывая ни въ текстъ, ни въ таблицу № 10, исключительно пользуясь тѣми семью буквами ключа, которыя намъ уже извѣстны. Въ самомъ дѣлѣ, зная 7 рядовъ, мы знаемъ 7 начальныхъ буквъ ихъ, т. е. 0,7 того слова, которое служитъ ключемъ, а этого, надо думать, вполнѣ достаточно, чтобы его угадать: . ачальн . . ъ=начальникъ.

Составивъ, обычнымъ путемъ, квадратную табличку на базисѣ этого ключа (табл. № 12), прочитаемъ слѣдующее:

Таблица № 12.

	1	2	3	4	5	6	7	8	9	0
1	н	о	п	р	с	т	у	ф	х	ц
2	а	б	в	г	д	е	ж	з	и	і
3	ч	ш	щ	ъ	ы	ь	ѣ	э	ю	я
4	а	б	в	г	д	е	ж	з	и	і
5	л	м	н	о	п	р	с	т	у	ф
6	ь	ѣ	э	ю	я	а	б	в	г	д
7	н	о	п	р	с	т	у	ф	х	ц
8	н	і	й	к	л	м	н	о	п	р
9	к	л	м	н	о	п	р	с	т	у
0	ъ	ы	ь	ѣ	э	ю	я	а	б	в

„Высокая фигура Николая сѣрѣла и уменьшалась, словно тая въ сѣрой мглѣ; еще минута, и онъ навсегда скрылся въ той темной дали, откуда неожиданно пришелъ, и уже ничего живого не видѣлось въ безлюдномъ пространствѣ".

Здѣсь мы сохранили въ текстѣ букву ъ, потому что она существуетъ и въ шифрѣ. Иначе мы имѣли бы большой плюсъ въ смыслѣ разгадки. Если бы въ текстѣ не было твердыхъ знаковъ, то на подсчетной таблицѣ (табл. № 10) — нижняя лѣвая клѣтка (01), соотвѣтствующая послѣдней буквѣ ключа, стояла бы пустая, а это сейчасъ бы навело насъ на мысль, что тутъ надо предполагать ъ (или ь). Пустынный характеръ нижняго ряда лишь подкрѣпилъ бы наше предположеніе, и, такимъ образомъ, отсутствіе Ъ въ криптограммѣ на за что, ни про что дало бы намъ цѣлый рядъ.

Продолжая изучать подсчетную таблицу, мы наткнемся на одно интересное и весьма существенное для всей категоріи квадратныхъ шифровъ явленіе. Мы увидимъ, что первый вертикальный столбецъ выдѣляется изъ всѣхъ остальныхъ отсутствіемъ пустыхъ клѣтокъ и вообще своей полнотой, которая лучше всего выразится, если мы суммируемъ клѣтки каждаго столбца въ отдѣльности и сравнимъ между собою результаты. Окажется, что сумма

въ 1-мъ	столбцѣ	—	32	въ 6-мъ	столбцѣ	—	21
„ 2	„		17	„ 7	„		12
„ 3	„		14	„ 8	„		14
„ 4	„		18	„ 9	„		12
„ 5	„		22	„ 0	„		7

Это явленіе объясняется отчасти тѣмъ, что первый столбецъ, будучи крайнимъ слѣва, находясь, такъ сказать, подъ рукою, чаще бросается въ глаза при шифрованіи, и потому безсознательно имъ чаще пользуются. Но главная причина заключается въ специфическомъ характерѣ (въ разбираемой системѣ) перваго столбца. Въ то время, какъ всѣ остальные содержатъ въ себѣ совершенно случайный, нечленораздѣльный составъ буквъ — первый, наоборотъ, представляетъ *слово*, т. е. естественное благозвучное сочетаніе, для котораго необходима правильная пропорція и распредѣ-

174, а онѣ вѣдь распредѣляются между 100 знаками. Чѣмъ больше зашифрованныхъ буквъ, тѣмъ картина выступаетъ рельефнѣе.

леніе гласныхъ, употребительныя буквы и т. д. Пропорція перворазрядныхъ буквъ здѣсь будетъ, по необходимости, весьма высокая, между тѣмъ какъ въ другихъ она можетъ оказаться гораздо незначительнѣе, да и распредѣленіе будетъ нелѣпое. Напр., третій столбецъ (см. табл. № 12) заключаетъ въ себѣ буквы: п, в, щ, в, н, э, и, й, м, ь, изъ коихъ, по настоящему, только одна перворазрядная (н). То же самое и въ четвертомъ столбцѣ: р, г, ъ, г. *о*, ю, р, к, *н*, ѣ, и во всѣхъ остальныхъ (въ ключѣ *семь* перворазрядныхъ!). Это обстоятельство служитъ для отличія сложнаго квадратнаго отъ простого, о чемъ рѣчь въ слѣдующей главѣ.

Сравнивая подсчетную таблицу (табл. № 10) съ табличкой развернутаго ключа (табл. № 12), мы можемъ прослѣдить, какъ часто и равномѣрно пользовались разными значеніями одной и той же буквы. Буква *а*, напр., имѣетъ четыре значенія: 21, 41, 66, 08; и вотъ первыя два встрѣчаются по 4 раза, а вторыя два по 3 раза; такое распредѣленіе—чрезвычайно равномѣрное, даже идеальное, и подобное мы замѣтимъ и по отношенію къ остальнымъ буквамъ. Ясно, что писавшій былъ чрезвычайно внимателенъ во время шифрованія и добросовѣстно старался использовать всѣ знаки равномѣрно. Въ дѣйствительности же поступаютъ далеко не такъ тщательно. Шифрующій, во-1-хъ, зачастую совершенно не видитъ того, что пишетъ, но и помимо того, даже если бы онъ и стремился къ равномѣрной утилизаціи знаковъ, онъ не былъ бы въ состояніи этого добиться, потому что при писаніи невозможно держать въ памяти движеніе сотни знаковъ и помнить, сколько разъ каждый уже былъ въ дѣйствіи; наконецъ, обыкновенно и не задаются такой цѣлью, а шифруютъ, какъ попало, выхватывая знаки изъ таблицы, гдѣ придется; благодаря этому одни обозначенія какой-либо буквы встрѣчаются часто, другія же рѣдко. На таблицѣ № 13 сдѣланъ подсчетъ знаковъ, послѣ того, какъ тотъ же самый текстъ былъ зашифрованъ по тому же ключу человѣкомъ малоопытнымъ, не видѣвшимъ того, что пишетъ. Разница противъ таблицы № 10 довольно значительная.

Таблица № 13.

	1	2	3	4	5	6	7	8	9	0
1	1	4	—	—	3	—	—	—	—	—
2	6	1	5	3	4	6	2	—	—	—
3	2	2	1	2	1	—	—	—	—	—
4	4	—	2	1	1	5	1	1	3	—
5	6	5	4	5	1	3	4	4	1	—
6	2	1	—	1	4	3	—	—	—	1
7	4	2	1	—	3	2	4	1	—	—
8	7	—	3	2	4	—	2	1	—	2
9	2	—	—	3	4	—	2	1	1	—
0	4	1	1	5	—	—	—	1	—	2

Спрашивается, когда же дешифрированіе легче: въ томъ ли случаѣ, если стараются утилизировать знаки равномѣрно, или когда объ этомъ вовсе не думаютъ? Нетрудно сообразить, что чѣмъ больше стараются о равномѣрности, тѣмъ выходитъ... *хуже*, ибо характеристическія особенности горизонтальныхъ рядовъ на подсчетной таблицѣ выступаютъ отчетливѣе, а стало быть болѣе предательски. Но, конечно, безсознательное отношеніе къ процессу записыванія нисколько не поправляетъ дѣла; зачастую съ перваго же взгляда можно узнать по высокому коэффиціенту буквы *о*, *а*.., а слѣдовательно и весь соотвѣтствующій рядъ.

Отмѣтимъ, кстати, одну ошибку, которую часто дѣлаютъ по незнанію. Часто встрѣчаются скопленія буквъ, которыя можно найти всѣ или почти всѣ въ одномъ ряду таблицы. Соблазняясь такимъ удобнымъ положеніемъ, пишущій, не мудрствуя лукаво, такъ и беретъ буквы изъ одного ряда. Это даетъ сочетанія, весьма выгодныя для разгадки. Положимъ, напр., что мы добрались до значенія 5-го ряда (табл. № 12) и мы находимъ въ текстѣ сочетаніе: 57585456125359, гдѣ, кромѣ одной, всѣ буквы принадлежатъ 5 му ряду. Подставляя, получаемъ: стор. ну = сторону, что даетъ значеніе 12, т. е. значеніе перваго ряда. Отсюда понятно правило, котораго нужно держаться въ квадратныхъ шифрахъ: заботиться, чтобы не происходило скопленій чиселъ изъ одного и того же ряда. То же слово правильно было бы зашифровать такъ: 57169574881159.

Если разсмотрѣть слово „начальникъ" съ точки зрѣнія пригодности его быть ключомъ квадратнаго шифра, то его никоимъ образомъ нельзя назвать плохимъ, ибо онъ для перворазрядныхъ буквъ даетъ много комбинацій. Къ сожалѣнію, ходячіе ключи весьма часто заставляютъ желать много лучшаго. Придумать недурной ключъ вещь довольно трудная, а обыкновенно раздумываютъ недолго, при томъ имѣя самое смутное представленіе объ употребляемости буквъ. Нерѣдко ключи такъ нераціо-

нальны, что для высшихъ буквъ имѣется всего по 2-3 значенія, а для рѣдкихъ по 4-5. Въ нашей задачѣ текстъ былъ зашифрованъ по таблицѣ изъ 10×10 клѣтокъ, но легко понять, что если бы она заключала и 20×20, то уменьшилась бы только яркость подсчетной таблицы: число пустыхъ клѣтокъ возросло бы, въ прочихъ коэффиціенты понизились бы, но относительное распредѣленіе по прежнему было бы типичнымъ, а потому раскрытіе было бы, быть можетъ, не такимъ быстрымъ, но все же неизбѣжнымъ.

Заключеніе. Ясно, что простой квадратный шифръ совершенно непригоденъ; это одна изъ самыхъ неудачныхъ системъ, а между тѣмъ, стыдно сказать, она больше всего въ ходу. Даже многоклѣточныя таблицы при малыхъ текстахъ ненадежны, но онѣ къ тому же требуютъ много времени для составленія и потому не совсѣмъ удобны.

Глава V.

СЛОЖНЫЙ КВАДРАТНЫЙ ШИФРЪ.

Пришлося брать наживу съ бою.
И дологъ, и жестокъ былъ бой на этотъ разъ.

Крыловъ.

Предыдущая система, какъ мы убѣдились, имѣетъ два крупныхъ недостатка. Съ одной стороны, *распредѣленіе* знаковъ между буквами безусловно нецѣлесообразное, а съ другой—и это еще хуже—*расположеніе* ихъ въ таблицѣ необыкновенно примитивно: они просто идутъ въ алфавитномъ порядкѣ. Уничтожить этотъ второй, наиболѣе вредный недостатокъ имѣетъ цѣлью сложный квадратный шифръ. Это достигается при помощи введенія *распредѣлителя*.

Возьмемъ слово изъ 10 буквъ: „квадратный". Подъ той буквой, которая въ азбукѣ стоитъ ближе всего къ началу, поставимъ единицу; въ нашемъ случаѣ ее придется написать подъ *а*; подъ той буквой, которая въ азбукѣ стоитъ ближе всего къ первой б квѣ, поставимъ 2. Въ нашемъ случаѣ ее придется поставить подъ второй *а*, такъ какъ во взятомъ словѣ ея имѣется два экземпляра. Подъ буквой *в* придется 3; подъ *д*—4; подъ *й*—5 и т. д.

к в а д р а т н ы й.
6 3 1 4 8 2 9 7 0 5.

Получается число, содержащее 10 различныхъ цифръ, порядокъ которыхъ зависитъ отъ взятаго слова. Оно то и будетъ *распредѣлителемъ*.

Положимъ, что съ помощью этого распредѣлителя намъ нужно видоизмѣнить порядокъ въ десятибуквенномъ рядѣ, расположенномъ по алфавиту:

л, м, н, о, п, р, с, т, у, ф.

Выпишемъ наше число и подъ единицей подпишемъ первую букву — *л*, подъ 2—*м*, подъ 3—*н*, и т. д.:

6 3 1 4 8 2 9 7 0 5.
р н л о т м у с ф п.

Рядъ буквъ сталъ теперь неузнаваемымъ. Таковъ принципъ сложнаго квадратнаго шифра.

Таблица составляется такъ. Пусть ключомъ будетъ слово „шампанское“ (помимо прежняго слова „квадратный“, которое будетъ у насъ распредѣлителемъ). Составимъ обычный квадратъ изъ 10×10 клѣтокъ и надпишемъ сверху числовой распредѣлитель (табл. № 14), а подъ его цифрой 1 подпишемъ вертикально ключъ. Верхній рядъ начинается съ буквы *ш*; онъ, слѣдовательно, будетъ содержать слѣдующія 10 буквъ: ш, щ, ъ, ы, ь, ѣ, э, ю, я, а. Распредѣлимъ ихъ по вышеописанному способу, т. е. подъ 1—ш, подъ 2—щ, подъ 3—ъ и т. д. То же самое продѣлаемъ и со 2-мъ рядомъ и со всѣми остальными. Когда покончимъ съ послѣднимъ, десятымъ рядомъ, зачеркнемъ распредѣлительное число и сверху надпишемъ обыкновенный рядъ чиселъ отъ единицы до десяти (нуля). Такимъ же образомъ пронумеруемъ и горизонтальные ряды (слѣва). Таблица готова.

Таблица № 14.

	1	2	3	4	5	6	7	8	9	0
	6	3	1	4	8	2	9	7	0	5
1	ѣ	ъ	*ш*	ы	ю	щ	я	э	а	ь
2	е	в	*а*	г	з	б	и	ж	і	д
3	с	о	*м*	п	у	н	ф	т	х	р
4	ф	с	*п*	т	ц	р	ч	х	ш	у
5	е	в	*а*	г	з	б	и	ж	і	д
6	т	п	*н*	р	ф	о	х	у	ц	с
7	ц	у	*с*	ф	ш	т	щ	ч	ъ	х
8	п	м	*к*	н	с	л	т	р	у	о
9	у	р	*о*	с	х	п	ц	ф	ч	т
0	й	з	*е*	и	л	ж	м	к	н	і

Записываются буквы изъ нея такъ же, какъ и при простомъ квадратѣ: для *а* имѣемъ 3 значенія: 19, 23, 53; для *ф* пять значеній: 37, 41, 65, 74, 98.

Другіе составляютъ таблицу иначе. Пишутъ ключъ и остальныя буквы таблицы совершенно такъ, какъ и при простой квадратной системѣ, и послѣ сверху надписываютъ распредѣлительное число (табл. № 15). Буква *ш* по этой таблицѣ изобразится: 16, 45 77; буква д—28, 58.

Таблица № 15.

	6	3	1	4	8	2	9	7	0	5
1	*ш*	щ	ъ	ы	ь	ѣ	э	ю	я	а
2	*а*	б	в	г	д	е	ж	з	и	і
3	*м*	п	о	п	р	с	т	у	ф	х
4	*п*	р	с	т	у	ф	х	ц	ч	ш
5	*а*	б	в	г	д	е	ж	з	и	і
6	*н*	о	п	р	с	т	у	ф	х	ц
7	*с*	т	у	ф	х	ц	ч	ш	щ	ъ
8	*к*	л	м	н	о	п	р	с	т	у
9	*о*	п	р	с	т	у	ф	х	ц	ч
0	*е*	ж	з	и	і	й	к	л	м	н

При первомъ способѣ составленія таблицы раньше пишется распредѣлитель, а потомъ уже по немъ наносятся буквы; при второмъ—распредѣлитель выписывается послѣ того, какъ буквы уже нанесены въ алфавитномъ порядкѣ. Мы назовемъ первый способъ—*первичнымъ*, второй—*вторичнымъ* Ясно, что приготовить таблачку вторичнымъ способомъ значительно проще, зато пользоваться ею при писаніи и чтеніи писемъ нѣсколько менѣе удобно, ибо глазъ привыкъ наверху искать цифры на ихъ естественныхъ мѣстахъ, а вмѣсто того тамъ онѣ находятся въ необычномъ сочетаніи.

На первый взглядъ кажется, что этимъ мелкимъ обстоятельствомъ и исчерпывается все различіе между таблицами, составленными тѣмъ и другимъ способомъ, что это—различіе чисто техническаго свойства, въ родѣ того, напр., пишутъ ли раньше письмо, а потомъ заполняютъ адресъ на конвертѣ, или наоборотъ. Въ дѣйствительности же, какъ это ни покажется страннымъ, при томъ же ключѣ и распредѣлителѣ, криптограммы нѣтъ возможности прочесть, если получатель, по незнанію, составитъ таблицу не тѣмъ способомъ, по какому написано письмо. Въ самомъ дѣлѣ, сравнимъ между собою знаки однѣхъ и тѣхъ же буквъ изъ обѣихъ таблицъ:

	Буква *а*.	Буква *і*.	Буква *ф*.
Первичный способъ (табл. № 14):	19, 23, 53	29, 59, 00	37, 41, 65, 74, 98.
Вторичный способъ (табл. № 15):	15, 26, 56	25, 55, 08	30, 42, 67, 74, 99.

Соотвѣтственныя пары всѣ оказываются тождественными исключительно въ *первой* своей цифрѣ, указывающей на номеръ горизонтальнаго ряда. Что касается второй цифры, обозначающей столбецъ и связанной съ распредѣлителемъ, то она со-

всѣмъ не совпадаетъ на обѣихъ таблицахъ. Ясно, что вторая таблица имѣетъ совершенно другой распредѣлитель, чѣмъ первая. И дѣйствительно, съ точки зрѣнія послѣдней, распредѣлитель на табл. № 15 будетъ не 6314829705, а другое число, находящееся въ довольно своеобразной зависимости отъ прежняго. Чтобы его получить, надо въ нашемъ числѣ *совершить обмѣнъ между каждой цифрой и мѣстомъ ея въ числѣ;* напр., цифра 6 стоитъ на 1-омъ мѣстѣ, поэтому надо 1 поставить на 6-мъ мѣстѣ; цифра 3 стоитъ на 2-омъ мѣстѣ, поэтому надо 2 поставить на 3-ьемъ мѣстѣ; цифра 7 стоитъ на 8-омъ мѣстѣ. поэтому 8 надо поставить на 7-омъ, и т. д. Такимъ образомъ получимъ новое число 3624018579. Слѣдовательно, если отправитель писалъ по распредѣлителю: „квадратный", а получатель знаетъ только вторичный способъ составленія таблицы, то ему надобно надписать сверху не то число, которое даетъ условное слово, а его производное, составленное по указанному закону.

Намъ ни разу не пришлось встрѣтить среди товарищей знакомство съ этимъ обстоятельствомъ. Обыкновенно, когда уславливаются о шифрированной перепискѣ по сложной квадратной системѣ, ограничиваются сообщеніемъ ключа и словеснаго распредѣлителя. Поэтому, если оба корреспондента „учились" не у одного ментора, т. е. привыкли къ разнымъ способамъ нанесенія таблицы, то нерѣдко получатель, тщетно побившись надъ таинственнымъ текстомъ, въ отчаяніи рѣшаетъ, что его корреспондентъ по ошибкѣ взялъ не тотъ ключъ или распредѣлитель. Намъ извѣстны случаи, когда вслѣдствіе этого приходилось и удавалось искусственно расшифровать письмо и найти распредѣлитель, который, конечно, оказывался совсѣмъ не тѣмъ, чѣмъ условленный (т. е., напр., вмѣсто 6314829705, соотвѣтствующаго слову „шампанское", получалось 3624018579, источникъ котораго былъ совершенно непонятенъ). И курьезно, что во всѣхъ тѣхъ случаяхъ, о которыхъ мы знаемъ, никому ни разу не приходило въ голову, какъ просто открывается ларчикъ.

Ясно, что, во избѣжаніе такихъ недоразумѣній, необходимо, кромѣ ключа и распредѣлителя, условиться и относительно способа составленія.

Мы до сихъ поръ постоянно говорили о таблицѣ изъ 10×10 клѣтокъ, но ихъ можетъ быть и больше. Способъ записыванія текста будетъ тогда или въ видѣ дробей, или посредствомъ вставки нулей, или какъ-нибудь иначе (см. предыдущую главу).

Особенности системы. Примѣненіе этого шифра на практикѣ весьма удобно и только немногимъ сложнѣе простого квадратнаго. Что касается разгадки, то тутъ дѣло несравненно труднѣе; тамъ одна угаданная буква кладетъ лоскомъ цѣлый рядъ, чѣмъ наносится смертельный ударъ, здѣсь она остается изолированной, и побѣда кажется все такъ же проблематичной.

Задача. 13462822081529628207501655323766831237472308187240794438560460 6
2013128²1404856559804727042845313268 40 ²7025756538132408292712506428220395408 9
08171004⁶6062691620043703480445743703422865677312448047121031158740637464483 2
5266722304501984850888310435659208951654876281 3882625274101328924863010405081
8622265 ⁵7674316631038730097093787989398013748204152607942037041307441529038 55
3693236462849406372748198074758122203274138744539628382288954074240363798196 5
0174050852762849404804930923253780700394440860042474874904963 1 286863481259628
5082766437204841597122945041623401062220357 32³260860398666...

Распознаваніе системы. По общему виду криптограммы, по тому, что число цифръ въ ней четное *), и по характеру двузначныхъ чиселъ, на которыя ее разо-

---

*) Четность или нечетность цифръ имѣетъ вообще большое значеніе для распознаванія. Замѣтимъ, что если шифруютъ не все письмо, а отдѣльныя фразы, чередующіяся съ контекстомъ (а такъ поступаетъ огромное большинство пишущихъ), то значеніе четности-нечетности становится почти рѣшающимъ, ибо она опредѣляется не однократно, а во многихъ самостоятельныхъ участкахъ; въ случаѣ, напр., квадратнаго шифра *во всѣхъ* участкахъ обязательно должно быть по четному числу цифръ. Вообще, ходячій способъ несплошной шифровки сильно облегчаетъ раскрытіе, но объ этомъ см. глав. XVIII.

бьемъ (отъ 11 до 00), сейчасъ видно, что имѣемъ дѣло съ квадратнымъ шифромъ. Для того же, чтобы узнать, съ какой формой его, составимъ обычную подсчетную таблицу (табл. № 16). Если бы это былъ *простой* квадратный шифръ, то крайній лѣвый столбецъ долженъ былъ бы выдѣляться своей полнотой. Въ дѣйствительности, онъ какъ разъ наоборотъ поражаетъ своей пустынностью. Ясно, слѣдовательно, что это не простой, а сложный квадратный. Конечно, могло бы случиться и такъ, что 1-ый столбецъ былъ бы достаточно полный, и онъ дѣйствительно соотвѣтствовалъ бы ключу, и все-таки это былъ бы не простой, а сложный. Это бываетъ въ тѣхъ рѣдкихъ случаяхъ, когда первая цифра распредѣлителя — единица. Шифръ былъ бы принятъ тогда за простой квадратный, но съ первыхъ же шаговъ ошибка раскрылась бы.

Таблица № 16

	1	2	3	4	5	6	7	8	9	0
1	—	7	4	1	4	3	1	2	2	4
2	—	6	5	2	2	3	4	9	4	2
3	6	5	1	—	2	3	6	4	3	1
4	1	2	1	4	4	2	5	5	3	8
5	—	3	1	2	1	1	1	1	2	3
6	—	8	4	2	6	5	1	2	2	4
7	—	4	1	10	1	2	—	2	2	3
8	2	4	2	2	4	1	4	—	3	4
9	—	2	2	2	2	1	1	2	—	—
0	3	—	9	15	2	—	5	11	2	—

Раскрытіе шифра. Принимаемся за тщательное изученіе таблицы № 16, на которой разнесены всѣ 290 буквъ текста. Раньше всего необходимо добраться до того, въ какомъ столбцѣ скрывается ключъ. Мы уже знаемъ, что въ немъ обыкновенно бываетъ много перворазрядныхъ и мало рѣдкихъ буквъ. Изъ всѣхъ 10 столбцовъ наибольшей солидностью отличается второй; въ немъ шесть клѣтокъ имѣютъ числа 4—8 и лишь одна пустая. Но даже сама эта пустая клѣтка служитъ доказательствомъ правильности сдѣланнаго нами выбора. Она помѣщается въ концѣ столбца и наводитъ поэтому на мысль, что здѣсь въ ключѣ стоитъ *ъ*, который въ текстѣ вездѣ опускался, вслѣдствіе чего клѣтка 20 вышла пустая. Такіе случаи на практикѣ бываютъ сплошь и рядомъ. Отсюда прямой выводъ, что нижній рядъ есть рядъ буквъ, начинающійся съ *ъ* и кончающійся *в*. Но мы, однако, въ дальнѣйшемъ не воспользуемся своей легкой побѣдой, потому что, если бы въ ключѣ не было *ъ*, или если бы въ текстѣ онъ не опускался, то этого лишняго козыря мы бы не имѣли. Во всякомъ случаѣ, болѣе чѣмъ вѣроятно, что ключъ скрывается во второмъ столбцѣ, иначе говоря, единица распредѣлителя *) помѣщается во второмъ столбцѣ, что мы выразимъ такъ: № 2=I. Вообще, въ дальнѣйшемъ изложеніи мы для краткости будемъ обозначать вертикальные столбцы арабскими цифрами подъ № (№ 1, № 2...), цифры распредѣлителя — римскими (I, II...), а горизонтальные ряды арабскими цифрами со знакомъ § (§ 1, § 2...).

Для уясненія послѣдующаго разбора важно замѣтить себѣ вотъ что. Отъ введенія распредѣлителя буквы въ горизонтальныхъ рядахъ ужъ не идутъ въ алфавитномъ порядкѣ, но нисколько не уничтожается та особенность, что каждый рядъ заключаетъ въ себѣ отдѣльный *сплошной* (т. е. безъ пропусковъ) десятибуквенный участокъ азбуки. Среди этихъ сплошныхъ участковъ обязательно должно быть нѣсколько центральныхъ (т. е. группирующихся вокругъ *о*): безъ этихъ буквъ не можетъ обойтись ни одно длинное слово. Но также обязательно долженъ быть и рядъ, *начинающійся* съ буквы *а*. Дѣло въ томъ, что въ таблицѣ („развернутомъ ключѣ") должно же содержаться нѣсколько экземпляровъ этой перворазрядной буквы. Но такъ какъ она есть первая буква азбуки, то она можетъ попасть въ таблицу или тогда, когда она имѣется въ самомъ ключѣ, или, по крайней мѣрѣ, когда въ ключѣ находятся какія-нибудь изъ конечныхъ буквъ азбуки: ш, щ... (ср. табл. № 15, первый рядъ). Однако, было бы крайне нерасчетливо, если бы источникомъ *всѣхъ* экземпляровъ *а* были только рѣдкія, послѣднія буквы въ ключѣ, ибо пропорція буквъ въ таблицѣ вышла бы ужъ слишкомъ нелѣпою. И дѣйствительно, намъ неизвѣстенъ ни одинъ ключъ квадратнаго шифра, въ которомъ не было бы *а*.

Дальнѣйшій анализъ будетъ довольно кропотливъ, почему потребуется со стороны читателя усиленное вниманіе.

Прежде всего намъ надлежитъ разыскать неизбѣжный рядъ *а*. Вспомнимъ, что этотъ рядъ заключаетъ 4 крупныя буквы: *а*, е, и, в, второразрядную *д*, мелкія

*) Вѣдь ключъ пишется подъ цифрой 1 распредѣлителя (см. табл. № 14).

б, г, ж, з и послѣднюю самую мелкую — і (ср. табл. № 5). Такой пропорціи удовлетворяетъ вполнѣ рядъ 6 (§ 6), въ которомъ есть числа: 8, 6, 5, 4, 4; 2, 2, 2, 1; и, наконецъ, пустая клѣтка. Подъ послѣдней, надо полагать, скрывается *і*, изъ чего выходитъ, что первый столбецъ (№ 1) соотвѣтствуетъ десятой цифрѣ распредѣлителя (ибо *і*, *десятая* буква ряда *а*, приходится на *первый* столбецъ). № 1=X. Второй и первый столбцы оказываются полярными столбцами: тамъ начала всѣхъ рядовъ, здѣсь — окончанія; знакъ 61=і; 62=а.

Просматривая таблицу съ расчетомъ, не окажется ли тамъ еще одинъ рядъ буквы *а*, натыкаемся на § 1, который вполнѣ аналогиченъ § 6: на тѣхъ же столбцахъ подъемы, на тѣхъ же и спуски; слѣдовательно, 11=і, 12=а. Ключъ, оказывается, начинается буквой *а*; очевидно, вторая буква его будетъ согласная. Но § 2, по своей полнотѣ и непрерывности, несомнѣнно центральный рядъ, а такъ какъ *конечная* клѣтка его (21) пустая, то это *ф*, изъ чего неизбѣжно слѣдуетъ, что начальная буква этого ряда (22) есть *л*. Въ этомъ ряду л, м, н о..... ф—самая крупная буква есть *о* и, повидимому, ей то соотвѣтствуетъ самая выдающаяся клѣтка 28. Но если это такъ, то восьмой столбецъ отстоитъ отъ второго всего на 4 клѣтки, ибо *о* четвертая буква, считая отъ *л*. Иными словами, № 8=IV. Итакъ мы знаемъ уже истинное отношеніе между тремя столбцами — і-ымъ, 2-ымъ и 8-ымъ; оно равно X:I:IV. Мы можемъ, поэтому, возвращаясь къ § 1 и § 6, установить, что 18 и 68, отстоящія отъ *а* на четыре буквы — представляютъ собою *г*.

Присмотримся теперь къ § 3. Здѣсь обѣ *полярныя* клѣтки, 31 и 32, судя по своимъ высокимъ коэффиціентамъ — перворазрядныя буквы. Во всемъ алфавитѣ есть только одна пара, е.....н, которая подходитъ подъ такое условіе; при такомъ предположеніи 32 (клѣтка ключа) будетъ *е*, что вполнѣ подходитъ, ибо предшествующая буква ключа была *л*. Къ тому же 38 тогда будетъ *и*, а въ таблицѣ мы находимъ на этомъ мѣстѣ соотвѣтственно большое число — 4. На этомъ предположеніи мы поэтому и останавливаемся.

Обратимся теперь къ тексту. Подъ (1) находимъ группу 31326840=пег.=него; 40=*о*, что вполнѣ подтверждается табл. № 16, гдѣ въ этой клѣткѣ стоитъ большое число — 8. Итакъ, § 4 есть рядъ *о*, начинающійся и оканчивающійся малыми буквами, и въ которомъ четвертая буква (48) — крупная, ибо выражается числомъ 5. Единственное подходящее сюда сочетаніе буквъ (ничего другого не можетъ быть) есть рядъ к, л, м, н, о.....у. Итакъ, 41=у; 42=л; 48=н, а № 10 оказывается V. Подѣлившись послѣднимъ пріобрѣтеніемъ съ прежними горизонтальными рядами, найдемъ, что 10 и 60 дадутъ *д* (пятую букву отъ *а*), 30=і (пятое мѣсто отъ *е*), 20=п (пятое мѣсто отъ *л*).

Въ текстѣ подъ (2) разыщемъ 6062013128 = *да . но=давно*: 01 = *в*, слѣдовательно, 02 (полярная клѣтка, конецъ ключа)=*ъ*; 08=*ѣ*; 00=*э*.

Подъ (3) группа: 2340106222035732 = *но дал . . е=дальше*: 03=*ь*; 57=*ш*.

Мы только что видѣли, что въ № 2 нижняго ряда находится ъ, а третья за нимъ по азбукѣ буква ь оказывается въ № 3; но № 2 соотвѣтствуетъ I, слѣдовательно, № 3=III; отсюда, обходя всѣ прежніе ряды, найдемъ, что 13=в; 23=н; 33=з; 43=м; 63=в. Нанесемъ для наглядности всѣ добытыя данныя на таблицу. (Таблица № 17).

Въ самомъ началѣ текста группа: 134 6282208=*в . олѣ*; такъ какъ *46* непремѣнно изъ ряда *о*, то в . олѣ = в полѣ; 46=п; это шестая буква, начиная съ начальной *к*, слѣдовательно, № 6=VI; отсюда 16=е; 26=р, и т. д. (См. табл. № 17).

Подъ (5): 0104050818622265=*в . . ѣгали =выбѣгали* (для неизвѣстныхъ двухъ знаковъ 04 и 05 весь выборъ заключался между *ы*, *я*, *а*, *б*). Отсюда № 4=II; № 5=IX. Дѣлаемъ соотвѣтственный расчетъ для всѣхъ извѣстныхъ намъ рядовъ.

Таблица № 17.

	1	2	3	4	5	6	7	8	9	0
1	і	а	в			е		г		д
2	ф	л	н			р		о		п
3	н	е	з			й		и		і
4	у	к	м			п		н		о
5										
6	і	а	в			е		г		д
7										
8										
9										
0	в	ъ	ь			ю		ѣ		э
	X	I	III			VI		IV		V

Подъ (6): 6428220395408908171004=боль . о. ѣзды = большой ѣзды; отсюда 95=ш; 89=й, и опять расчетъ для другихъ клѣтокъ § 9; сейчасъ за этимъ: 60626 916200437034804=да . е пы . ьны (для неизвѣстнаго 69 только выборъ между ж и з) =даже пыльны. И т. д., и т. д. Задача въ сущности давно рѣшена, тѣмъ болѣе, что давно уже можно было угадать весь ключъ: „Александръ". Распредѣлитель— 0132968475. Какому слову онъ соотвѣтствуетъ, узнать невозможно, если только для него не было взято то же слово, что и для ключа: это часто практикуется *). Разобранный текстъ гласитъ:

„Въ полѣ и садахъ еще лежалъ снѣгъ, но улицы давно были чисты отъ него, сухи и въ мѣстахъ большой ѣзды даже пыльны; только изъ палисадниковъ, обнесенныхъ желѣзными рѣшетками, да со дворовъ выбѣгали тоненькія струйки воды и расплывались лужей по ровному асфальту, и отъ каждой такой лужи въ обѣ стороны тянулись слѣды мокрыхъ ногъ, въ началѣ темные и частые, но дальше рѣдкіе..."

На таблицѣ № 18 представленъ полный развернутый ключъ. Примѣненъ былъ *первичный* способъ.

Таблица № 18.

	0	1	3	2	9	6	8	4	7	5
1	і	а	в	б	и	е	з	г	ж	д
2	ф	л	н	м	у	р	т	о	с	п
3	н	е	з	ж	м	й	л	и	к	і
4	у	к	м	л	т	п	с	н	р	о
5	ъ	с	у	т	щ	ц	ш	ф	ч	х
6	і	а	в	б	и	е	з	г	ж	д
7	ц	н	п	о	х	т	ф	р	у	с
8	м	д	ж	е	л	і	к	з	й	и
9	щ	р	т	с	ш	х	ч	у	ц	ф
0	в	ъ	ь	ы	б	ю	а	ѣ	я	э

Заключеніе. Нельзя отрицать, что сложный квадратный шифръ представляетъ для своей разгадки значительныя трудности. Онѣ въ высокой степени возрастаютъ, если текстъ невеликъ, если отъ слишкомъ безпорядочной, слишкомъ наивной шифровки подсчетная таблица выходитъ недостаточно рельефной, если при томъ тщательно слѣдить, чтобы знаки изъ одного горизонтальнаго ряда не помѣщались по сосѣдству, если ключъ подобрать искусно, если нарочно его столбцомъ пользоваться поменьше и т. д. Но съ другой стороны—нѣкоторыя изъ этихъ требованій не совсѣмъ совмѣстимы, а, главное, всѣ перечисленныя осложняющія обстоятельства теряютъ свое значеніе, разъ криптограмма представляетъ не единичный сплошной текстъ, а отдѣльные зашифрованные участки въ письмѣ. Основная бѣда этой системы заключается въ томъ, что въ горизонтальныхъ рядахъ находятся сплошные отдѣлы азбуки, и что законъ распредѣленія въ нихъ буквъ *одинаковъ для всѣхъ рядовъ*. Если мы добираемся до нѣкоторыхъ элементовъ этого закона для одного ряда, то мы тѣмъ самымъ дѣлаемъ пріобрѣтенія и для остальныхъ. Одно случайно угаданное или распознанное слово (а это при „оазисномъ" способѣ шифрованія бываетъ сплошь и рядомъ) для такихъ шифровъ то же, что для корабля подводная пробоина: онъ немедленно потонетъ. Ни разу еще не случилось, чтобы не удавалось расшифровать разбираемымъ способомъ записанные тексты, когда нужда заставляла этимъ заняться.

---

*) Здѣсь послужило слово „разбойники".

Глава VI.

ПРЕРЫВИСТЫЙ КВАДРАТНЫЙ ШИФРЪ.

(Съ фиктивными цифрами).

...Лишь дураки
Тутъ не увидятъ явнаго обмана.
Шекспиръ, „Ричардъ III".

Система, о которой будетъ трактоваться въ этой главѣ, по своему строенію не представляетъ почти никакого отличія отъ простого или сложнаго квадратнаго шифра, но зато она вводитъ совершенно новый элементъ—надувательскій, стремленіе сбить съ толку жандармовъ или, выражаясь вульгарно, „втереть имъ очки". На сцену выступаютъ *фиктивныя* цифры, которыхъ цѣль заключается въ томъ, чтобы сдѣлать текстъ недоступнымъ для расчлененія на отдѣльные знаки, т. е. на отдѣльныя двузначныя числа.

Пусть данъ ключъ изъ *восьми* буквъ: „моя щетка", и условлено считать фиктивными *двѣ* цифры, напр., 4 и 7. Составимъ квадратъ изъ 10×10 клѣтокъ, и *оставивъ пустыми 4-ый и 7-ой горизонтальные ряды, а также 4-ый и 7-ой вертикальные столбцы*, размѣстимъ въ остальныхъ клѣткахъ развернутый ключъ, по методу простого квадратнаго шифра (табл. № 19), послѣ чего проставимъ, по обыкновенному, сверху и слѣва послѣдовательный рядъ цифръ отъ 1 до 0. Такова будетъ таблица прерывистаго шифра.

Таблица № 19.

	1	2	3	4	5	6	7	8	9	0
1	*м*	н	о		п	р		с	т	у
2	*о*	п	р		с	т		у	ф	х
3	*я*	а	б		в	г		д	е	ж
4										
5	*щ*	ъ	ы		ь	ѣ		э	ю	я
6	*е*	ж	з		и	і		й	к	л
7										
8	*т*	у	ф		х	ц		ч	ш	щ
9	*к*	л	м		н	о		п	р	с
0	*а*	б	в		г	д		е	ж	з
	8	9	5		3	6		2	1	0

Легко видѣть, что въ знакахъ, которыми выражаются буквы по этой таблицѣ, цифры 4 и 7 совершенно отсутствуютъ.

Шифрованіе заключается въ томъ, что забирая изъ таблицы нужные знаки, пишущій въ то же время вставляетъ время отъ времени ту или другую изъ фиктивныхъ цифръ, а иногда обѣ вмѣстѣ. Напр., фраза: „письмо получено", по настоящему, могла бы быть изображена такъ: 1565905593211596602888081296. Съ фиктивными же цифрами картина мѣняется: 1456590755932415796640288778081297б.

Условныхъ фиктивныхъ цифръ можетъ быть и не двѣ, напр., одна или три.

Нѣтъ никакой необходимости составлять квадратъ изъ 10×10 клѣтокъ. Въ нашемъ случаѣ его можно было начертить изъ 8×8, но при пронумеровываніи надо обязательно пропустить фиктивныя цифры—4 и 7. (Ср. табл. № 20).

Очевидно, что тотъ же пріемъ примѣнимъ и къ сложному квадратному шифру. Распредѣлитель долженъ содержать столько же буквъ, что и ключъ, т. е. въ нашемъ случаѣ 8. Пусть это будетъ „столовая". Составимъ по немъ распредѣлительное число обычнымъ порядкомъ съ тѣмъ лишь различіемъ, что цифры 4 и 7 пропустимъ, такъ что съ 3 прямо перескочимъ на 5 и съ 6 на 8:

с т о л о в а я
8 9 5 3 6 2 1 0

Если дѣло затѣмъ идетъ о *вторичномъ* способѣ, то это число надписываемъ сверху надъ буквенными столбцами (минуя пустые; см. табл. № 19 *внизу*). Если же условлено по *первичному*, то раньше пишутъ число, а послѣ разносятъ буквы. На табл. № 20, сдѣланной по этому методу, пустые столбцы выброшены, такъ что слѣва нумерація идетъ съ пропускомъ 4 и 7; то же самое и сверху въ числовомъ ряду, замѣняющемъ зачеркиваемое распредѣлительное число.

Прерывистый шифръ сравнительно мало извѣстенъ, но употребляется.

Особенности системы. Вставка фиктивныхъ цифръ уничтожаетъ всю обычную методику раскрытія квадратныхъ шифровъ. Основной подготовительный процессъ — подсчетъ знаковъ становится невозможнымъ, ибо двузначныя числа, замѣняющія буквы, ужъ не прилегаютъ вплотную другъ къ другу, а разорваны, разъединены, разобщены одно отъ другого элементами, похожими на нихъ, какъ двѣ капли воды, которые, поэтому, невозможно ни распознать, ни удалить. Примѣненіе этого шифра весьма удобно, но криптограмма отъ вставки постороннихъ цифръ получается значительно удлиненной.

Таблица № 20.

	1	2	3	5	6	8	9	0
	8	9	5	3	6	2	1	0
1	с	т	п	о	р	н	*м*	у
2	у	ф	с	р	т	п	*о*	х
3	д	е	в	б	г	а	*я*	ж
5							*ш*	
6		и	т.	д.			*е*	
8							*т*	
9							*к*	
0							*а*	

Задача. 0218459618237178565431329261356274328519231512001435192095692316572708662295432186453447815073020417545424875594020328120331573095832135772795982776926388398051557204443241873405332849157739563462672213510682190050842630409120534459328747635884625030376569126991592363451911270540215498812370873548517184588128321135400514 7...

Распознаваніе системы. Если какая-нибудь система основана на обманѣ или фокусѣ, то распознаваніе ея получаетъ особое значеніе: зачастую это — половина рѣшенія задачи, нерѣдко — *все*. Нѣтъ ни одной системы, въ которой способъ писанія шифрованнаго текста игралъ бы большую роль, чѣмъ здѣсь, въ смыслѣ и діагноза системы, и опредѣленія числа фиктивныхъ цифръ, и раскрытія этихъ послѣднихъ. Можно смѣло сказать, что быстрота рѣшенія прямо пропорціональна квадрату, если не кубу, количества отдѣльныхъ шифрованныхъ участковъ. Въ то время, какъ написанныя оазисным способомъ криптограммы (по разбираемой системѣ) намъ удавалось и распознать, и прочитать въ какой-нибудь часъ, — сплошная криптограмма зачастую требуетъ много кропотливаго труда.

Часто достаточно вглядѣться въ способъ писанія *цифръ*, чтобы распознать систему. Даже и неопытный глазъ замѣтитъ, что въ обыкновенныхъ квадратныхъ системахъ цифры группируются парами, хотя бы пишущій и старался писать ихъ слитно. Это происходитъ просто отъ того, что написавши двузначное число и обращаясь въ таблицѣ для разысканія слѣдующей буквы, онъ дѣлаетъ невольный перерывъ, послѣ котораго опять разомъ наноситъ двузначное число; къ тому же онъ часто предыдущаго знака уже и не видитъ. Мало того: шифрующій почти всегда, дойдя до края строки, совершенно безсознательно старается *не* раздѣлять двузначнаго числа, не разрывать его, вслѣдствіе чего въ большинствѣ строкъ, если не во всѣхъ, окажется четное число цифръ; и еще болѣе: многіе даже *слово* стѣсняются разрывать, и почти всегда у нихъ начало строки совпадаетъ съ началомъ слова. Все это нарушается только тогда, когда сперва пишутъ черновикъ, а съ него уже механически и поспѣшно снимается копія.

Въ прерывистомъ шифрѣ дѣло обстоитъ иначе. Благодаря вставкѣ или приставкѣ фиктивной цифры къ двузначному числу, взятому изъ таблицы, цифры наносятся или группируются не только парами, но и тройками; число цифръ въ строчкѣ никоимъ образомъ не будетъ всегда четнымъ. Вообще внѣшній видъ опытному глазу сразу бросается въ глаза, особенно, когда написано оазисно. Намъ случалось видѣть, — замѣчаемъ для курьеза, — такія, напр., фразы: „Посылку изъ 491 получилъ... Вчера арестованъ 857“.

Далѣе, въ то время, какъ въ обыкновенныхъ квадратныхъ шифрахъ число *цифръ* обязательно четное, какъ во всей криптограммѣ, такъ и въ *каждомъ* зашифрованномъ участкѣ, какъ бы малъ онъ ни былъ (и нерѣдко и въ каждой строчкѣ), здѣсь эта обязательность совершенно исчезаетъ. Напр., въ нашей „задачѣ“ число *цифръ* 323. Разсовывая свои фиктивныя цифры, пишущій рѣшительно не въ состояніи контролировать ихъ и нормировать; онъ вполнѣ рабъ своей системы. Если письмо состоитъ изъ одного зашифрованнаго участка, то 50% шансовъ, что окажется нечетное число; если же нѣсколько, то всѣ 100%.

Вообразимъ, однако, случай, правда, чрезвычайно рѣдкій, когда имѣется всего

единичный сплошной текстъ съ *четнымъ* числомъ цифръ, и притомъ переписанный съ черновика, стало быть безъ характеристичныхъ особенностей — можно ли тогда распознать систему? Вполнѣ возможно и тогда. Кое что можетъ дать подсчетъ въ текстѣ каждой *цифры* въ отдѣльности, т. е. опредѣленіе количества единицъ, двоекъ, троекъ и т д. Дѣло въ томъ, что въ обыкновенномъ квадратномъ шифрѣ относительныя количества ихъ, хотя и различны и даже допускаютъ значительныя отступленія отъ средней величины, но все же предѣлы качаній ихъ не такъ ужъ велики; напр., для таблицы № 16 мы имѣемъ такія данныя:

Цифры . . .	1,	2,	3,	4,	5,	6,	7,	8,	9,	0.
Количества .	*40*,	*77*,	62,	75,	43,	55,	53,	64,	34,	76.

Въ прерывистомъ же, гдѣ источникъ фиктивныхъ цифръ совсѣмъ иной, чѣмъ остальныхъ, гдѣ все зависитъ отъ каприза пишущаго, возможны, конечно, самыя чудовищныя уклоненія въ ту или другую сторону.

Затѣмъ, если текстъ по обыкновенному способу разбить на *грани* изъ двухъ цифръ и составить подсчетную таблицу, то картина получится безцвѣтная и мало типичная для квадратнаго шифра: клѣтки будутъ выполнены гораздо равномѣрнѣе, ибо фиктивными цифрами разрушаются естественныя пары и создаются новыя. Наконецъ, въ силу этого послѣдняго обстоятельства окажется, что тѣ двузначныя числа, которыя чаще всего встрѣчаются въ текстѣ, весьма часто не совпадаютъ съ гранями, иначе говоря, отстоятъ нерѣдко другъ отъ друга на нечетное число цифръ. Напр., въ нашей „задачѣ" самыя частыя двузначныя числа:

32	встрѣчается	9	разъ,	совпадаетъ съ гранями	5	разъ
51	„	8	„	„ „	3	„
54	„	8	„	„ „	4	„

Для сравненія выберемъ изъ текста предыдущей главы тоже 3 самыя частыя двузначныя числа:

04	встрѣчается	18	разъ,	совпадаетъ съ гранями	15	разъ
74	„	14	„	„ „	10	„
08	„	12	„	„ „	11	„

Раскрытіе шифра. Когда мы убѣдились, что передъ нами прерывистый шифръ, является вопросъ, сколько въ немъ фиктивныхъ цифръ: одна, двѣ или три. Собственно говоря, три цифры — дѣло совсѣмъ невѣроятное: въ этомъ случаѣ таблица содержала бы всего $7 \times 7 = 49$ знаковъ, т. е. менѣе, чѣмъ полторы азбуки. При такомъ ничтожномъ количествѣ знаковъ получилась бы неизбѣжно самая нелѣпая пропорція буквъ: къ тому же тремя фиктивными цифрами орудовать хлопотливо: пишущій обязательно либо недосолитъ, либо пересолитъ; наконецъ, криптограмма при этомъ чудовищно растянется, на каждую букву придется по 3-4 цифры. Итакъ, рѣчь можетъ итти только объ одной или двухъ цифрахъ. При оазисномъ способѣ писанія вопросъ рѣшается весьма быстро посредствомъ разсчета четныхъ и нечетныхъ цифръ; одновременно же опредѣляются и самыя цифры.

Предполагаемъ сперва, что имѣется всего 1 фиктивная цифра и пусть въ одномъ участкѣ изъ 187 цифръ окажется:

1,	2,	3,	4,	5,	6,	7,	8,	9,	0
15,	*21*,	*26*,	*19*,	*22*,	*23*,	*18*,	*16*,	*15*,	*12*

Разъ сумма нечетная, то виновата въ этомъ фиктивная цифра, которая, очевидно, встрѣчается сама нечетное число разъ. Слѣдовательно таковой можетъ быть одна изъ 5 цифръ: 1, 2, 4, 6, 9.

Изъ другого участка мы можемъ получить, напр., такой выборъ: 3, 6, 7, 0, изъ чего сразу опредѣлится, что искомая цифра — *6* (какъ общая обоимъ результатамъ). Если же окажется противорѣчіе, если результаты будутъ исключать другъ друга, то ясно будетъ, что имѣются *двѣ* фиктивныя цифры, которыя нетрудно будетъ найти по такому же способу.

Мы даемъ теперь общій методъ выдѣленія фиктивныхъ цифръ, пригодный и для единичнаго сплошного текста. Вотъ его основаніе. Число знаковъ при прерывистомъ шифрѣ сильно уменьшено противъ обычнаго: при 2 фиктивныхъ цифрахъ мы имѣемъ всего $8 \times 8 = 64$ клѣтки вмѣсто 100. Ясно, что важнѣйшіе знаки будутъ сильно повторяться. Пишущій чувствуетъ это, боится этого и на нихъ устремляется

его вниманіе. Къ нимъ-то онъ присосѣживаетъ большей частью свои фиктивные знаки, разбивая ими злополучныя пары и стараясь сдѣлать ихъ неузнаваемыми. Если, напр., фиктивными цифрами являются 4 и 7, а повторяются 32 и 95, то онъ пишетъ: ...342...975...495...732...372...945... Во всѣхъ случаяхъ прерывистаго шифра, съ которыми мы встрѣчались, мы всегда замѣчали это любопытное, хотя и легко объяснимое явленіе. Такимъ образомъ, при самомъ тѣсномъ, непосредственномъ участіи той или другой фиктивной цифры образуется множество трехзначныхъ чиселъ, которыя, очевидно, будутъ неоднократно повторяться, ибо повторяется источникъ ихъ — опредѣленныя пары. Если, стало быть, ихъ выдѣлить и подвергнуть анализу, то можно будетъ добраться до фиктивныхъ цифръ.

Составимъ изъ текста нашей „задачи" всѣ возможныя трехзначныя числа; ихъ будетъ столько, сколько тамъ цифръ безъ двухъ, т. е. 321. Сдѣлать это нетрудно. Выпишемъ начало текста: 021845961823..... Первое число — 021; подвинувшись на одну цифру вправо, получаемъ 218, затѣмъ 184, 845, 459, 596 и т. д. Всѣ трехзначныя числа размѣстимъ въ порядкѣ отъ 000 до 999 и обозначимъ сбоку въ скобкахъ, сколько разъ каждое встрѣчается. (Табл. № 21).

Таблица № 21.

000	100	200	300	400	500	600	700	800	900
001	106	200	302	400	502	613	705	805	900
005(2)	112	203(2)	304	402(2)	507	618	708(2)	812(3)	911
014	113	204(2)	309	405	508	622	717	815	912(2)
020(2)	120(3)	205	313	409	510	625	718	821	920
021(2)	123	209	315(2)	417	512	626	720	823	923(3)
030	126	211	316	418	513	627	722	827	926(2)
032	127	213(2)	321(3)	424	514	630	727(2)	832(2)	932
033	128	215	324	426	515	634	730	839	940
037	130	218(2)	328(4)	432(3)	517	635	734	842	954
040	132	219	329	433	519(3)	638	735	845(2)	956(2)
041	135(4)	221	331	435	533	645	739	846	958
044	143	229	332	443	534(2)	654	743	849	959
050	147	231(2)	341	444	540(2)	656	747	851(2)	961
051(2)	150	236	344(2)	445	542	657	754	856	980
053(2)	151(2)	237(2)	351(2)	447	543(2)	662	755	864	982
054	154	241	354(2)	451	545	672	763	866	988
068	155	248	356	453	548	682	765	873	991
073	157	250	357	454	549	691	769	874	
084	159	263(3)	358	458	557	692(2)	772	875	
086	165	267	361	459(2)	559(2)		773(2)	881(2)	
087	171	269	370	462(2)	562		776	883	
091	175	270	371	476	563		781	884	
095(2)	178	274	376	478	565		785		
	183	277	388	485	569		795		
	184	279	395	487	572(2)				
	186	281	398	492	577(2)				
	187	283		498	583				
	190	284			588(2)				
	191	285			592				
	192(2)	287			593				
					594				
					596				
					598				

Соберемъ всѣ повторяющіяся трехзначныя числа въ одну табличку. (Табл. № 22).

Таблица № 22.

Повторяющіяся 2 раза.					Повторяющіяся 3 раза.	Повторяющіяся 4 раза.
005	203	351	559	845	120	135
020	204	354	572	851	263	328
021	213	402	577	881	321	
051	218	459	588	912	432	
053	231	462	708	926	519	
095	237	534	727	956	812	
151	315	540	773		923	
192	344	543	832			

Чтобы разобраться въ этой табличкѣ, подсчитаемъ, сколько разъ принимаютъ участіе въ образованіи трехзначныхъ чиселъ единицы, сколько—двойки и т. д.

Окажется, что:

1,	2,	3,	4,	5,	6,	7,	8,	9,	0
18,	*24,*	*19,*	*11,*	*22,*	*5,*	*5,*	*9,*	*10,*	*12*

Если бы своимъ коэффиціентомъ одна цифра рѣзко выдѣлялась изъ остальныхъ, то это была бы единственная фиктивная цифра, что могло бы сейчасъ же быть подкрѣплено разсчетомъ четности. У насъ же этого нѣтъ, поэтому беремъ двѣ максимальныя цифры 2 и 5, которыя, вѣроятно, и суть таинственные незнакомцы. Чтобы убѣдиться окончательно въ этомъ, посмотримъ, сочетаются ли онѣ другъ съ другомъ въ трехзначныхъ числахъ табл. № 22. Если онѣ дѣйствительно фиктивны, то онѣ весьма мало или вовсе не должны совмѣстно встрѣчаться въ нихъ, ибо каждая троица образуется отъ внѣдренія *одной* фиктивной въ пару нефиктивныхъ. Для наглядности выберемъ самыя частыя цифры; кромѣ 2 и 5 таковыми окажутся 1 и 3.

Какъ часто сопрягаются между собою эти четыре цифры—мы увидимъ изъ таблички № 23. Самое большее число даютъ 2 и 3; минимальное—2 и 5.

Таблица № 23.

	2	3	5
1	9	6	8
2		10	1
3			7

Итакъ, фиктивныя цифры опредѣлены. Теперь остается ихъ изгнать, и наша криптограмма отъ этой операціи сильно порѣдѣетъ. Вотъ истинный текстъ:

0184961837178643139613674381931100143190969316770866943186434478107300417444879400381033173098313777998776963883980170444344187340338491773963466713106819000846304091034493874763884603037669169919363419117040149881370873481718488183113400147.

Тутъ оказывается всего 120 знаковъ или буквъ. Составимъ подсчетную таблицу (табл. № 24). Наиболѣе полнымъ столбцомъ является первый вертикальный (въ немъ изъ 8 буквъ—пять крупныхъ), слѣдовательно, надо предположить простой квадратный. Расправа, поэтому, весьма короткая. Рядъ 3, несомнѣнно, начинается съ *а* (подъемы на *в*, *е*). Ряды 8 и 9 — центральные, въ послѣднемъ буква *о* приходится, повидимому, на 96 (высшая клѣтка), слѣдовательно, рядъ=л, м, н, о, п, р, с, т. Въ восьмомъ— 89, вѣроятно, *ф*, слѣдовательно, рядъ = о, п, р, с, т, у, ф, х. Возьмемъ въ текстѣ недалеко отъ начала группу: 331730983137779987769638=б. зрад. ст. ое=безрадостное; слѣдовательно 17=е; 77 = о; 76=н. Пріобрѣли, значитъ, еще два ряда, и т. д.

Таблица № 24.

	1	3	4	6	7	8	9	0
1	1	3	1	1	4	2	—	3
3	6	1	4	—	3	5	—	2
4	3	4	3	—	1	—	3	2
6	—	2	—	3	1	—	1	1
7	2	2	2	2	2	1	—	2
8	3	1	3	2	4	2	—	—
9	3	3	2	5	—	2	1	2
0	4	1	2	1	—	1	1	4

Разобранный текстъ гласитъ: „И рождество въ этомъ богатомъ домѣ наступило смутное и безрадостное. Присутствіе человѣка, который ни въ чемъ не раздѣлялъ мыслей и чувствъ окружающихъ...“

Ключъ: „басъ коли“. Присутствіе въ немъ *ъ* и отсутствіе его въ текстѣ объясняетъ пустую клѣтку въ ключѣ (61). Развернутый ключъ нанесенъ на таблицѣ № 25.

Заключеніе. Разсмотрѣнная система представляетъ хорошій примѣръ того, что въ шифрахъ съ однимъ желаніемъ „провести“ далеко не уѣдешь. Тѣ ухищренія, которыя корреспонденты придумываютъ для усложненія дѣла и заметенія слѣдовъ системы, кажутся имъ совсѣмъ новыми, никому невѣдомыми, въ дѣйствительности же это только одинъ самообманъ. Поразительно часто корреспонденты напоминаютъ страусовъ, прячущихъ въ песокъ свою голову и увѣренныхъ, что никто ихъ не видитъ.

Несомнѣнно, прерывистый квадратный шифръ никуда негоденъ; тотъ *плюсъ*, который онъ даетъ своими фиктивными цифрами, совершенно проблематиченъ, а между тѣмъ количество дѣйствительныхъ знаковъ въ развернутомъ ключѣ сильно уменьшается. Въ особенности наивно дѣтскимъ является пользованіе этимъ шифромъ при *оазисномъ* записываніи.

Таблица № 25.

	1	3	4	6	7	8	9	0
1	б	в	г	д	е	ж	з	и
3	а	б	в	г	д	е	ж	з
4	с	т	у	ф	х	ц	ч	ш
6	ъ	ы	ь	ѣ	э	ю	я	а
7	к	л	м	н	о	п	р	с
8	о	п	р	с	т	у	ф	х
9	л	м	н	о	п	р	с	т
0	и	і	й	к	л	м	н	о

Глава VII.

МНОЖЕСТВЕННЫЙ КВАДРАТНЫЙ ШИФРЪ.

По идеѣ своей множественный квадратный шифръ не отличается особенной глубиной. Вмѣсто того, чтобы пользоваться однимъ ключомъ и одной таблицей квадратной системы, составляютъ ихъ нѣсколько, напр., 2, 3, 4, и затѣмъ при шифрованіи берутъ знаки сначала изъ 1-й таблицы, потомъ изъ 2-й, 3-й и т. д.: наконецъ, возвращаются опять къ первой и, такимъ образомъ, періодически обходятъ всѣ развернутые ключи. Положимъ, напр., что ключами служатъ слова: „эта коробка“, „начальникъ“, „александръ“. Составляемъ три таблицы (по простой квадратной системѣ, см. табл. 9, табл. 12 и табл. 26). Пусть нужно зашифровать фразу: „Письмо получено. Не отвѣчалъ все время, ибо сомнѣвался въ адресѣ“. Прежде чѣмъ пользоваться этой системой, надо условиться о „переходѣ“ съ одного ключа на другой.

Таблица № 26.

	1	2	3	4	5	6	7	8	9	0
1	а	б	в	г	д	е	ж	з	и	і
2	л	м	н	о	п	р	с	т	у	ф
3	е	ж	з	и	і	й	к	л	м	н
4	к	л	м	н	о	п	р	с	т	у
5	с	т	у	ф	х	ц	ч	ш	щ	ъ
6	а	б	в	г	д	е	ж	з	и	і
7	н	о	п	р	с	т	у	ф	х	ц
8	д	е	ж	з	и	і	й	к	л	м
9	р	с	т	у	ф	х	ц	ч	ш	щ
0	ъ	ы	ь	ѣ	э	ю	я	а	б	в

Безъ условнаго перехода получатель будетъ даромъ терять время, стараясь понять смыслъ начинающейся нескладицы, пока не догадается, что пора переходить къ слѣдующей таблицѣ. Этотъ условный знакъ, очевидно, не долженъ быть впѣшнимъ, ибо тогда система потеряетъ почти весь свой raison d'être. Онъ можетъ быть только *внутреннимъ*, на который натыкаются въ процессѣ чтенія. Таковымъ можетъ быть какое-нибудь короткое условное слово, но гораздо лучше двукратное или трехкратное повтореніе одной и той же буквы, конечно, выраженной въ разныхъ знакахъ, напримѣръ, 126209=ббб; 374188=ккк (табл. № 26). Понятно, что обыкновенно для этого прибѣгаютъ къ болѣе рѣдкимъ буквамъ, ибо перворазрядныя и безъ того часто эксплуатируются.

Выше приведенная фраза, взятая какъ примѣръ, можетъ быть зашифрована такъ: 460962934572514290681994714436245878725823043141920015264356185078314307 190924514543716001189156581481316013561196285.

Если ее при помощи ключей перевести обратно на общепонятный языкъ, то найдемъ слѣдующее:

„Письмо получено не ххх отвѣчал все врфффемя, ибо сомнѣвалдддся в адресѣ".

Таблицы можно условиться составлять или по *простой* квадратной системѣ, или по *сложной*, или, наконецъ, часть по одной, часть по другой. Соотвѣтственно этому у насъ будетъ одна изъ трехъ формъ:

1) Множественный простой квадратный шифръ,
3) Множественный сложный квадратный шифръ,
3) Множественный смѣшанный квадратный шифръ.

Особенности системы. На первый взглядъ можетъ показаться, что все дѣло заключается только въ томъ, что вмѣсто одной сотни клѣтокъ мы получаемъ въ свое распоряженіе нѣсколько сотенъ; буквы текста находятъ свое выраженіе въ значительно большемъ количествѣ знаковъ; соотвѣтственно уменьшается повторяемость каждаго и возрастаетъ поэтому трудность раскрытія. Однако, если бы это было такъ, то множественный простой (а отчасти и сложный) квадратный шифръ по существу вовсе не отличался бы отъ такого обыкновеннаго простого шифра, въ которомъ ключъ состоитъ изъ 20—30—40 буквъ: въ одномъ случаѣ три таблицы по 10×10 клѣтокъ, въ другомъ одна таблица въ 30×10 клѣтокъ; посвящать этой системѣ спеціальный разборъ и отдѣльную главу совсѣмъ не стоило бы; „улучшеніе" напоминало бы анекдотическую „усовершенствованную швейную машину", которая разсылалась желающимъ за 1 рубль и оказывалась обыкновенной иглой, но съ непомѣрно большимъ ушкомъ. Въ дѣйствительности же прогрессъ выходитъ весьма значительный, ибо количество здѣсь переходитъ въ качество.

Положимъ, что имѣемъ 3 таблицы по 100 клѣтокъ; тѣ же 300 будемъ имѣть и при простомъ квадратномъ шифрѣ изъ 30×10. Однако, разница существенная. Въ послѣднемъ случаѣ для нихъ существуютъ 300 различныхъ знаковъ, отъ 11 до 300: каждая клѣтка имѣетъ свой особый знакъ. Въ первомъ же случаѣ для нихъ оказывается только сотня знаковъ отъ 11 до 00; 300 клѣтокъ посылаютъ свои полномочія ста знакамъ; одинъ и тотъ же знакъ въ разныхъ таблицахъ. а стало быть и въ разныхъ частяхъ текста, выражаетъ неодинаковыя буквы; напримѣръ, 21 на таблицѣ № 9 —*т*, на таблицѣ № 12—*а*, на таблицѣ № 26—*л*. На криптограммѣ не замѣтно швовъ, не видно, что она составлена изъ многихъ разношерстныхъ участковъ, она кажется

Таблица № 27. Задача.

1	32898569152267890878	26	79257848577048777176
2	50874052389498562933	27	27615275883826725920
3	83528711515362073287	28	74917559066044487825
4	55852956025599821453	29	26432300533853988929
5	80728449680767393295	30	83356398285997890852
6	82027937649576706996	31	80598627821591269800
7	85056176376284907709	32	33425968957883458798
8	64766905162685671537	33	50511439789156629145
9	08678692139681298891	34	92066279927767529900
10	88860187678483686560	35	11848897619202870162
11	72004857116926395176	36	16272661929463620026
12	78072016504476227104	37	75887836729646849071
13	53051849567978274670	38	61749163192059494126
14	71767402677854487048	39	46707559724176569948
15	51081235586381835691	40	22047529514881377859
16	05628628394066875574	41	78990906780743760324
17	56836325278683917338	42	54226209836927722900
18	82832668559135806760	43	86806998964091265565
19	83686576788886926599	44	83996282995556679230
20	05174605678481849467	45	91881042568328860899
21	95260376190460722588	46	90001879376485832705
22	67846295268583716777	47	77051122877681167281
23	83859192620267846076	48	99738201697788819077
24	04678638798870167284	49	35509596001376813705
25	13422017487876057218	50	61421826668886920838

вполнѣ однородной, гомогенной, поэтому никакъ нельзя знать, гдѣ 21 перестаетъ быть *т* и начинаетъ изображать *а*, гдѣ кончаетъ обозначать *л* и возвращается опять къ *т*. Разбираемая система не можетъ быть уже названа „постояннозначной"; она „перемѣннозначна", хотя и въ зачаточной формѣ, ибо отдѣльные участки текста въ своихъ предѣлахъ постояннозначны.

Такимъ образомъ, отнимая у шифрующихъ столько же времени, сколько и длинный обыкновенный квадратный шифръ, разбираемая система несравненно надежнѣе. Остается только убѣдиться, абсолютна ли эта надежность и окупается ли ею нѣкоторая неуклюжесть и сложность шифра: составлять всякій разъ нѣсколько табличекъ не совсѣмъ пріятная вещь, въ особенности людямъ, ведущимъ большую переписку.

Задача. Дана довольно большая сплошная криптограмма изъ 500 буквъ (1000 цифръ). Въ виду того, что пользованіе нѣсколькими таблицами и выборъ нѣсколькихъ ключей даетъ слишкомъ много простору субъективному моменту, мы прямо воспользовались готовой комбинаціей ключей, въ томъ видѣ, какъ она примѣнялась недавно по этой системѣ группой товарищей для переписки; соотвѣтственно съ этимъ азбука взята здѣсь тюремная (см. глав. I). Шифрованіе поручено товарищу, чуждому всякой предвзятости.

Текстъ мы избрали въ видѣ таблички изъ 50 рядовъ по 20 цифръ (10 буквъ) въ каждомъ и перенумеровали ряды; такое заблаговременное расположеніе избавитъ насъ отъ необходимости совершить эту нужную операцію послѣ. Въ размѣрахъ текста нѣтъ ничего необычнаго. На этихъ дняхъ мы видѣли два письма, зашифрованныхъ по этой системѣ. Въ одномъ было 376 буквъ, въ другомъ 879!

Распознаваніе системы. Общій видъ криптограммы, четность цифръ и т. п. заставляютъ предполагать квадратый шифръ. Для дальнѣйшаго діагноза составляемъ подсчетную таблицу (см. табл. № 28). Нельзя отрицать, что картина получается совсѣмъ необычная. Пустыхъ и рѣдкихъ клѣтокъ совсѣмъ мало. Ряды сравнительно равномѣрно заполнены, какъ будто всюду центральные отдѣлы. Ни одна система, ни изъ разсмотрѣнныхъ уже, ни изъ описанныхъ въ слѣдующихъ главахъ, не дастъ подобной картины. Такой видъ ея объяснить нетрудно. При нѣсколькихъ ключахъ знаки, рѣдкіе въ одной табличкѣ, оказываются употребительными въ другой и наоборотъ. Въ результатѣ вершины и долины сглаживаются въ значительной степени, и получается нѣчто равномѣрное. Такимъ образомъ, распознаваніе можетъ быть сдѣлано безошибо но.

Раскрытіе шифра. Во множественномъ шифрѣ текстъ состоитъ изъ разношерстныхъ отрывковъ. Эти отрывки могутъ быть мелкими или крупными въ зависимости отъ того, какъ часто пишущій переходитъ отъ одного ключа къ другому. Однако, они не могутъ быть слишкомъ мелкими, ибо, во-первыхъ, слишкомъ хлопотливо постоянно переходить съ одной таблицы на другую, а съ другой стороны, благодаря необходимости всякій разъ дѣлать вставки для обозначенія „перехода", сильно возрасталъ бы объемъ криптограммы. Если бы дѣлать переходы, напр., въ среднемъ послѣ каждыхъ 10 буквъ, то при трехъ условныхъ буквахъ для сигнала, текстъ возросъ бы на 30 %. Если въ письмѣ 300 буквъ, то вставныхъ потребуется 90, т. е. 30 группъ по 3 одинаковыхъ буквы. При томъ такое большое число своеобразныхъ буквенныхъ сочетаній дастъ большой козырь при раскрытіи, какъ будетъ показано ниже. Въ большинствѣ зашифрованныхъ описываемымъ путемъ писемъ, которыя намъ случалось видѣть, размѣры лоскутовъ доходили до 35-50 и болѣе буквъ. Изъ упомянутыхъ выше двухъ писемъ одно при 879 буквахъ состояло изъ 22 лоскутовъ, т. е. по 40 буквъ въ среднемъ, другое, писанное человѣкомъ, предупрежденнымъ о необходимости какъ можно чаще дѣлать переходы, при 376 буквахъ, содержало 16 лоскутовъ, т. е. по 24 буквы въ каждомъ. Хорошо ли, если отдѣльныя звенья достигаютъ такой величины? Намъ извѣстно, что въ 1000 бук-

Таблица № 28.

	1	2	3	4	5	6	7	8	9	0
1	4	1	3	2	3	5	2	4	2	1
2	—	5	1	1	4	13	7	3	6	4
3	—	3	2	—	3	1	6	6	5	1
4	2	4	2	2	2	4	—	9	3	3
5	5	5	5	2	6	9	2	1	7	4
6	6	1	4	3	5	2	15	5	7	5
7	5	10	2	4	5	15	7	14	6	6
8	8	6	15	10	7	10	8	11	4	4
9	12	9	—	3	6	5	2	6	9	4
0	3	5	2	4	10	3	4	6	3	8

вахъ содержится въ среднемъ 112 разъ *о*, т. е. по одному *о* на $8^1/_2$ буквъ; при тюремной же азбукѣ одно *о* на 8 буквъ. Квадратный ключъ (изъ 10×10) даетъ въ среднемъ 3 буквы *о*, слѣдовательно, достаточно, чтобы лоскутъ содержалъ больше 24 буквъ, для того, чтобы въ немъ оказалось четвертое *о* и пришлось одинъ изъ 3 знаковъ повторить. Прибавимъ къ этому, что, во-первыхъ, ключи зачастую бываютъ возмутительно скверно выбраны, во-вторыхъ, если и при одной таблицѣ трудно контролировать утилизацію всѣхъ знаковъ, и часть одинаковыхъ обозначеній для одной и той же буквы мало замѣчается, то тѣмъ болѣе это бываетъ при нѣсколькихъ таблицахъ. Въ-третьихъ, въ живомъ языкѣ часто бываютъ большія скопленія одной и той же буквы на маломъ пространствѣ, вслѣдствіе чего рѣшительно неизбѣжны повторенія, напр.: „Варшава, Марталковская, Далаю". Здѣсь въ 25 буквахъ находится 8 *а*; въ одномъ мѣстѣ бываютъ скопленія одной буквы, въ другомъ — иной; онѣ отнюдь не распредѣлены равномѣрно. Наконецъ, способъ давать сигналы тремя знаками одной буквы тоже ухудшаетъ дѣло: если брать для этого рѣдкія буквы (ф, х, ц...), то будутъ невольно повторяться одинаковыя группы, если же брать болѣе употребительныя буквы, напр., такую, какая въ этомъ отрывкѣ уже имѣется, то искусственно создается повтореніе знаковъ. Напр., въ какомъ либо участкѣ уже имѣется буква *в* подъ знакомъ 13 (таблица № 26). Желая вернуться къ первому ключу, мы даемъ сигналъ *ввв* въ видѣ 136300, вслѣдствіе чего получилось повтореніе знака *13*.

Таблица № 32.

	1	2	3	4	5	6	7	8	9	0
1	1	—	—	2	2	—	—	1	—	1
2	—	2	—	—	1	3	3	3	4	—
3	—	3	2	—	1	—	2	3	4	1
4	—	2	—	—	2	—	—	—	1	3
5	2	3	3	—	6	7	—	1	3	2
6	—	5	2	2	2	1	4	3	3	—
7	—	2	1	1	—	—	—	3	2	—
8	1	5	10	1	2	5	5	1	4	4
9	8	2	—	1	2	1	1	6	4	1
0	—	2	—	—	1	1	2	3	1	3

Изъ всего сказаннаго достаточно явствуетъ, что каждый лоскутъ будетъ обязательно заключать въ себѣ повторные знаки, каковыми будутъ по преимуществу являться употребительныя буквы. Но каждый изъ взятыхъ развернутыхъ ключей обладаетъ различнымъ строеніемъ: употребительныя буквы въ одномъ выражаются совершенно иными знаками, чѣмъ въ другомъ. Отсюда ясно, что и характеръ повторяемости будетъ различенъ на лоскутахъ, соотвѣтствующихъ разнымъ ключамъ. Послѣ этихъ предварительныхъ замѣчаній можно уже вернуться къ нашей задачѣ.

Таблица № 33.

	1	2	3	4	5	6	7	8	9	0
1	2	—	3	—	1	4	1	1	1	—
2	—	1	—	—	1	6	2	—	1	1
3	—	—	—	—	1	1	3	2	—	—
4	—	2	—	—	—	2	—	1	—	—
5	—	1	—	—	—	—	2	—	—	1
6	4	6	1	1	3	1	10	2	3	4
7	1	5	1	—	1	8	6	2	2	2
8	6	1	5	9	5	5	3	9	—	—
9	2	7	—	2	4	4	1	—	3	3
0	3	2	1	2	7	—	—	2	1	4

Для того, чтобы заставить выступить наружу различіе строенія разныхъ участковъ, слѣдуетъ весь текстъ развернуть въ формѣ ленты. По настоящему надо было бы составить прямоугольникъ изъ 500×100 клѣтокъ. У узкаго бока его расположить 100 знаковъ текста (отъ 11 до 00), у широкаго выписать послѣдовательный рядъ чиселъ отъ 1 до 500, такъ какъ въ криптограммѣ нашей 500 буквъ. Затѣмъ оставалось бы отмѣтить для каждаго знака на его горизонтальномъ ряду тѣ клѣтки, которыя ему принадлежатъ сообразно тѣмъ мѣстамъ, на которыхъ данный знакъ встрѣчается въ текстѣ.

Въ виду того, однако, что такая таблица заняла бы огромную площадь, мы взяли для горизонтальнаго ряда не 500 клѣтокъ, а только 50, т. е. по десяти буквъ въ каждой. И все же намъ пришлось представить таблицу въ видѣ двухъ половинъ: таблицъ №№ 29 и 30 *).

*) См. въ концѣ книги.

Таблица № 29 показываетъ положеніе въ текстѣ первыхъ 50 знаковъ (отъ 11 до 50). Сверху нанесены числа, обозначающія нумерацію десятковъ буквъ текста. Нахожденіе даннаго знака въ соотвѣтственномъ десяткѣ обозначено посредствомъ стоячей палочки; двойная палочка указываетъ, что въ десяткѣ данный знакъ повторяется два раза.

Таблица № 34.

	1	2	3	4	5	6	7	8	9	0
1	—	1	—	—	—	1	1	2	1	—
2	—	2	1	1	2	4	2	—	1	3
3	—	—	—	—	1	—	1	1	1	—
4	2	—	2	2	—	2	—	8	2	—
5	3	1	2	2	—	2	1	—	4	1
6	2	—	1	—	—	—	1	—	1	1
7	4	3	—	3	4	7	1	9	2	4
8	—	—	—	—	—	—	—	1	—	—
9	—	—	—	—	—	—	—	—	2	—
0	—	1	1	2	2	2	2	1	1	1

Уже при поверхностномъ взглядѣ на табл. 29 и 30, особенно если соединить ихъ такъ, чтобы вторая составила продолженіе первой (по длинѣ), замѣчается въ расположеніи черточекъ какая-то правильность, какой-то нѣжный рисунокъ; можно ясно прослѣдить три-четыре вертикальныя волны. Это значитъ, что при зашифровываніи писавшій 3-4 раза обошелъ всѣ свои ключи. Мы замѣчаемъ, далѣе, что въ горизонтальныхъ рядахъ черточки распредѣлены неравномѣрно, а группируются довольно явственно въ нѣкоторыхъ пунктахъ. Для того, чтобы сдѣлать болѣе глубокій анализъ, выберемъ изъ обѣихъ таблицъ тѣ знаки, которые обладаютъ подобнаго рода скопленіями. Послѣ самаго краткаго изученія, мы ихъ расположимъ такъ, какъ на табл. 31*).

Волнистый рисунокъ выступаетъ на этой таблицѣ гораздо отчетливѣе, вмѣстѣ съ тѣмъ получается возможность различить отдѣльные лоскуты каждой волны. Въ отдѣлѣ A_1 видны скопленія въ 1-5 десяткахъ, а одновременно и въ 29-32 десяткахъ; отдѣлъ B: 5—10; 19—24; 33—37; 46—50; отдѣлъ C: 11—14; 25—28; 38—41. Отдѣлъ A_2, въ которомъ скопленія начинаются послѣ C въ 15-18 десяткахъ, и въ которомъ группы совпадаютъ съ A_1, очевидно, есть тотъ же отдѣлъ A_1, но лишь съ слабо выраженнымъ первымъ лоскутомъ. Наконецъ, отдѣлъ A/B есть смѣшанный, такъ какъ въ немъ одновременно имѣются скопленія и изъ A и изъ B. Число ключей—три. Мы получили, такимъ образомъ, въ грубомъ, неотдѣланномъ видѣ границы всѣхъ лоскутовъ. Вотъ они:

Ключъ I: 1—4½ дес.; 15—18; 29—32; 42—45.
Ключъ II: 4½—10; 19—24; 33—37; 46—50.
Ключъ III; 11—14; 25—28; 38—41.

Если бы даже дальнѣйшее, болѣе точное разграниченіе участковъ другъ отъ друга оказалось невозможнымъ, то и тогда задача была бы все равно рѣшена. Сложивши вмѣстѣ всѣ четные отрѣзки перваго ключа въ ихъ неотесанномъ, лапидарномъ видѣ, также 4 куска 2-го и три 3-го, мы получимъ три совершенно однородныхъ текста, изъ которыхъ каждый зашифрованъ на всемъ своемъ протяженіи одинаково. Однако, есть полная возможность увѣнчать зданіе, т. е. совершенно точно опредѣлить границы если не всѣхъ, то большинства лоскутовъ; для этого надо воспользоваться специфическимъ строеніемъ сигналовъ и постараться ихъ разыскать. Они обыкновенно состоятъ, какъ мы уже говорили, изъ трехъ разныхъ экземпляровъ одной и той же буквы. Слѣдовательно, первая ихъ особенность та, что это есть непремѣнно три буквы изъ *разныхъ рядовъ*, т. е. 3 двузначныхъ числа съ различной цифрой десятковъ, напримѣръ: 224380 = ммм (табл. № 26); 173283 = жжж; при этомъ пишутъ ихъ часто *сверху внизъ*. Вторая ихъ осебенность та, что всѣ три знака, выражая для соотвѣтствующаго ключа одну и ту же букву, обладаютъ приблизительно одной и той же употребляемостью въ составномъ, сшитомъ изъ всѣхъ своихъ лоскутовъ, текстѣ этого ключа. Наконецъ, подобнаго рода сочетанія неизбѣжно должны повторяться, какъ сигналъ, въ другомъ мѣстѣ текста, особенно при частыхъ переходахъ, ибо пишущему трудно запомнить, гдѣ какія буквы онъ бралъ въ качествѣ сигнала. Все это въ совокупности даетъ возможность точно найти границу. Въ нашемъ случаѣ, напримѣръ, группа 793764 въ шестомъ десяткѣ (см. „задачу", табл. № 27) повторяется и въ 46-омъ десяткѣ, въ обоихъ случаяхъ на границѣ между I и II ключами. Въ одинаковой употребляемости убѣждаются по подсчетнымъ таблицамъ, которыя составля-

*) См. въ концѣ книги.

ются, такъ сказать, предварительно для каждаго изъ трехъ сшитыхъ текстовъ; онѣ, впрочемъ, не могутъ сильно отличаться отъ истинныхъ (послѣднія нанесены на таблицахъ № 32 и № 34).

Для перваго текста, составленнаго изъ 4 лоскутовъ, мы имѣемъ 182 буквы. Это обыкновенный квадратный шифръ; судя по подсчетной таблицѣ (таблица № 32) —сложный. Разобрать его, конечно, особыхъ трудностей не составляетъ, тѣмъ болѣе, что выудивши сигналы, мы пріобрѣтаемъ нѣсколько весьма цѣнныхъ данныхъ: 79=37=64; 23=00=53 и т. д. Такимъ же образомъ можно будетъ совершенно самостоятельно раскрыть 2-ой и 3-ій тексты. Въ дѣйствительности же это сдѣлается еще легче, чѣмъ для перваго, потому что, прочитавъ 1-й лоскутъ, зашифрованный по 1-му ключу, мы уже по смыслу сообразимъ первое слово 2-го лоскута, а слѣдовательно, сдѣлаемъ широкую брешь во 2-мъ ключѣ; тѣмъ болѣе, что обыкновенно проницательные корреспонденты, воображая, что проявляютъ особую хитрость, стараются переходить съ одного ключа на другой на серединѣ слова, напр., „непремѣнно". (Ср. взятый нами примѣръ въ началѣ этой главы).

Число участковъ въ нашей задачѣ 11; размѣры ихъ таковы

Ключи	I	II	III
	55	50	
	35	64	39
	47	37	42
	45	44	42
Итого . .	182	195	123

Въ среднемъ на каждый участокъ приходится $45^1/_2$ буквъ.

Шифрами послужили слова: 1) Хвощинская, 2) Португалия, 3) Шахматисты. Всѣ они сложные квадратные, распредѣлителемъ для каждаго шифра служилъ его же ключъ; способъ *вторичный;* азбука тюремная. Текстъ составляетъ часть басни „Стрекоза и муравей".

Заключеніе. Нельзя отрицать, что разобранный шифръ принадлежитъ къ весьма труднымъ для разгадки системамъ. Если текстъ не очень большой, если ключи выбраны удачные, сложные квадратные, если слѣдятъ тщательно за утилизаціей всѣхъ знаковъ одной буквы, если переходы дѣлаютъ весьма часто, послѣ какихъ-нибудь 10—20 буквъ, а сигналы придумываютъ болѣе раціональные или просто обходятся безъ нихъ, то затрудненія для расшифровки становятся почти неодолимыми. Но все же увѣренности въ томъ, что шифръ не будетъ раскрытъ, у насъ не можетъ быть, да и не всегда выполненіе перечисленныхъ условій въ нашей власти (напр., величина текста). При оазисномъ же способѣ—неприступность шифра становится совсѣмъ проблематичной.

Если прибавить, что въ практическомъ отношеніи система эта не совсѣмъ удобна, ибо приходится запоминать нѣсколько ключей и всякій разъ составлять нѣсколько таблицъ, то слѣдуетъ придти къ заключенію, что мы еще очень далеки отъ идеала.

Глава VIII.

ПЕРІОДИЧЕСКІЙ РАЗДѢЛЬНЫЙ ШИФРЪ.

(Гамбеттовскій).

Живо дѣло закипѣло
И поспѣло въ полчаса.

Майковъ.

Предыдущая система до извѣстной степени можетъ уже быть названа перемѣннозначной. Теперь мы приступаемъ къ разсмотрѣнію настоящихъ представителей этого типа. Сущность гамбеттовскаго шифра заключается въ томъ, что живая рѣчь,

преобразованная въ числовой рядъ, видоизмѣняется числовымъ же ключомъ, накладываемымъ на нее послѣдовательно, періодически.

Положимъ, что нужно зашифровать фразу: „письма не получила". Подставимъ въ ней на мѣсто каждой буквы число, выражающее ея мѣсто въ азбукѣ (полной, см. главу I); получимъ рядъ: 17, 9, 19, 30, 14, 1, 15, 6, 17, 16, 13, 21, 25, 9, 13, 1. Пусть ключемъ будетъ слово „Европа", въ которомъ произведемъ такую же замѣну: 6, 3, 18, 16, 17, 1. Наложимъ ключъ на фразу столько разъ, сколько онъ на ней умѣстится, и произведемъ сложеніе вертикальныхъ паръ чиселъ:

Ключъ	6,	3,	18,	16,	17,	1.—	6,	3,	18,	16,	17,	1.—	6,	3,	18,	16...
Текстъ	17,	9,	19,	30,	14,	1,	15,	6,	17,	16,	13,	21,	25,	9,	13,	1...
Криптограмма .	23,	12,	37,	46,	31,	2,	21,	9,	35,	32,	30,	22,	31,	12,	31,	17

Таковъ періодическій раздѣльный шифръ, называемый обыкновенно гамбеттовскимъ и весьма употребительный. Мы называемъ его „раздѣльнымъ", потому что вслѣдствіе перемежающихся въ немъ двузначныхъ и однозначныхъ чиселъ ихъ приходится, во избѣжаніе путаницы, писать раздѣльно. Впрочемъ, можно писать и слитно, но тогда нужно передъ однозначными вставлять по нулю. Напр., предыдущій рядъ можетъ быть написанъ такъ: 231237463102210935323022341123117.

Эта система располагаетъ всего 67 знаками. Наименьшій 2 получается отъ наложенія двухъ *а* (1+1); наибольшій 68 — отъ сложенія двухъ *я* (34+34).

Особенности системы. Хотя число знаковъ здѣсь меньше, чѣмъ въ квадратномъ шифрѣ, но зато по сравненію съ послѣднимъ здѣсь есть громадное преимущество. Одинъ и тотъ же знакъ можетъ представлять совершенно различныя буквы, такъ какъ онъ могъ получиться отъ сложенія различныхъ чиселъ, напр., 10 можетъ быть суммой и 9+1, и 8+2, и 7+3, и т. д. Исключеніе составляютъ только крайніе знаки 2 и 68, которыя могутъ образоваться только однимъ путемъ. Во взятомъ нами образчикѣ мы видимъ, что 31 означаетъ послѣдовательно *м*, *ч*, *л*. Зато 12 въ обоихъ случаяхъ выражаетъ *и*, ибо случайно повторилось сочетаніе 3+9. Въ смыслѣ примѣненія разбираемую систему надо безусловно отнести къ числу весьма удобныхъ.

Задача. 27, 7, 28, 14, 52, 16, 21. 13, 9, 9, 21, 33, 25, 35, 49, 30, 25, 10, 32, 7, 19, 29, 48, 43, 13, 30, 2, 30, 7, 40, 34, 37, 17, 22, 28, 4, 9, 18, 17, 14, 52, 35, 18, 31, 2, 28, 24, 20, 33, 64, 49, 10, 27, 6, 26, 12, 47, 28, 43, 27, 25, 17, 10, 22, 35, 39, 34, 66, 33, 29, 18, 14, 41.

Распознаваніе системы. Діагносцируется гамбеттовскій шифръ съ перваго же взгляда: раздѣльность чиселъ и присутствіе среднихъ однозначныхъ выдаетъ его головой. Но если бы даже писали слитно (со вставкой нулей), то и тогда дѣло нисколько бы не затруднилось, благодаря тому, что знаки не выходятъ изъ границъ 2 и 68.

Раскрытіе шифра. Первымъ дѣломъ необходимо узнать, сколько буквъ въ ключѣ, иначе говоря — длину періода. Это будетъ нетрудно, если мы уяснимъ себѣ сущность разбираемой системы. Что такое ключъ? Рядъ разновеликихъ чиселъ, своеобразная кривая, гдѣ есть максимумъ и минимумъ. Вообразимъ этотъ ключъ многократно повтореннымъ одинъ за другимъ, получимъ цѣпь изъ одинаковыхъ звеньевъ. Если бы мы ее изобразили графически, то получили бы длинную кривую, составленную изъ одинаковыхъ частей, изъ одинаковыхъ волнъ. Если теперь на эту кривую наложить графически изображенный первоначальный текстъ (т. е. до измѣненія ключомъ), то характеръ кривой, конечно, въ высокой степени извратится, такъ что уже никоимъ образомъ нельзя будетъ распознать въ ней истинные, неизмѣненные изгибы и очертанія отдѣльной волны (т. е. періода, т. е. ключа), но *ширину* волны, количество буквъ въ ключѣ, возможно будетъ распознать съ достаточной точностью. Во взятомъ нами для примѣра ключѣ „Европа" — минимумъ есть 1, максимумъ — 18. Различныя буквы текста, падая на эти два крайніе полюса, могутъ въ большей или меньшей степени измѣнить ихъ взаимоотношеніе. Если, напр., на 1 упадетъ *я* (34), а на 18 — *л* (13), то бывшій минимумъ окажется даже больше бывшаго максимума. Но такое извращеніе бываетъ не часто. *Вообще*, какъ правило, характеръ полярныхъ знаковъ ключа пробьется непремѣнно — если не въ одной, такъ въ другой, третьей волнѣ. Поэтому стоитъ только изобразить въ формѣ кривой нашу

криптограмму,—и число буквъ ключа немедленно обнаружится съ достаточной ясностью. Табл. № 35 *) выполняетъ эту задачу.

Горизонтальныхъ линій въ ней 67 (2—68) по числу знаковъ, даваемыхъ гамбеттовскимъ шифромъ; вертикальныхъ 71 — столько, сколько буквъ въ „задачѣ". Легко видѣть, что спуски кривой приходятся на 27, 36, 45 и 54-ую буквы, а вершины на 5, 41, 50 и 68-ую буквы. Разстоянія между первыми 4 числами—9, 9, 9, а между послѣдними 36, 9, 18. Итакъ, не можетъ быть никакого сомнѣнія, что ключъ содержитъ 9 буквъ.

Разобьемъ нашу криптограмму на грани по 9 буквъ въ каждой и подпишемъ ихъ одну подъ другой. (Таблица № 36).

Таблица № 36.

I	II	III	IV	V	VI	VII	VIII	XI
27	7	28	14	52	16	21	13	9
9	21	33	25	35	49	30	25	10
32	7	19	29	48	43	13	30	2
30	7	40	34	37	17	22	28	4
9	18	17	14	52	35	18	31	2
28	24	20	33	64	49	10	27	6
26	12	47	28	43	27	25	17	10
22	35	39	34	66	33	29	18	14
41								

Что такое горизонтальные ряды этой таблички, мы уже знаемъ. Это волны, со своими максимумами и минимумами, наглядно представленныя на таблицѣ № 35. Что же такое вертикальные столбцы? Это, очевидно, совокупность чиселъ, получившихся отъ сложенія различныхъ буквъ текста съ *одной и той же* буквой ключа (мы для краткости говоримъ о сложеніи *буквъ* вмѣсто числовыхъ выраженій ихъ). Въ каждомъ вертикальномъ столбцѣ тоже имѣется свой минимумъ и максимумъ. Напримѣръ, въ первомъ столбцѣ наименьшее число—9, наибольшее — 41; очевидно, изъ девяти буквъ текста, составляющихъ первый столбецъ, первое число (9) образовано „малой" буквой (т. е. близкой къ началу алфавита), а второе число (41) — „большой" буквой.

Что даетъ намъ максимумъ столбца?

Возьмемъ для примѣра III столбецъ. Наибольшее число въ немъ 47 получилось отъ сложенія съ „большой" буквой. Если бы то было *я* (самая послѣдняя буква), то неизвѣстная буква ключа была бы 47—34=13. Если же не *я*, а меньшая буква, то буква ключа была бы не 13, а *больше*. Иными словами, максимумъ столбца даетъ намъ *минимумъ* для соотвѣтствующей буквы ключа.

Что же даетъ намъ минимумъ столбца? Въ томъ же третьемъ столбцѣ минимальное число—17. Оно получилось отъ сложенія съ „маленькой" буквой текста. Если бы то была *а*, то соотвѣтственная буква ключа была бы 17—1=16. Если же не *а*, а другая буква, то буква ключа была бы не 16, а меньше. Иными словами, минимумъ столбца даетъ *максимумъ* буквы ключа.

Ясно, что 3-я буква ключа содержится между 13 и 16.

Положимъ, что одна изъ восьми буквъ текста, приходящихся на III-ій столбецъ, есть *а*. Ясно, что она окажется въ минимумѣ столбца, т. е. въ 17, но тогда букву ключа мы можемъ сразу получить готовой: стоитъ только изъ 17 вычесть единицу (т. е. *а*). Но такъ какъ *а* весьма распространенная и потому, особенно при достаточномъ текстѣ, можетъ очутиться почти во всякомъ столбцѣ, то стоитъ только минумумъ каждаго столбца уменьшить на 1 и мы имѣемъ шансы получить буквы ключа. Выпишемъ минимумы:

Столбцы . . .	I,	II,	III,	VI,	V,	VI,	VII,	VIII,	IX.
Минимумы . .	9,	7,	17,	14,	35,	16,	10,	13,	2.
Числа ключа. .	8,	6,	16,	13,	34,	15,	9,	12,	1.
Буквы ключа. .	з	е	о	л	я	н	и	к	а.

*) См. въ концѣ книги.

Нетрудно догадаться, что искомый ключъ — „земляника". Поправку надо ввести только въ III-й столбецъ, гдѣ вмѣсто 16 истинное число — 14; Мы видимъ, что оно не выходитъ изъ выше опредѣленныхъ для III столбца предѣловъ: 13—16.

Когда ключъ найденъ, остается только для прочтенія криптограммы послѣдовательно вычитать знаки ключа изъ знаковъ текста. Получимъ: 19, 1, 14, 1, 18... Вотъ что мы прочтемъ: „Самара, Казанская улица, домъ графа Шувалова, квартира третья, Андрею Никодимичу Эртелю".

Врядъ ли долженъ спокойно спать г-нъ Эртель, адресъ котораго такъ мудро обезопасенъ.

Конечно, не всегда ключъ такъ легко опредѣляется. Иногда приходится довольно долго возиться надъ той или другой буквой его, пробуя между предѣльными для нея числами то или другое промежуточное. Это въ томъ случаѣ, если въ нѣсколько сосѣднихъ столбцовъ ни разу не попала буква *а* или, по крайней мѣрѣ, хоть *б* или *в*. Но, во всякомъ случаѣ, разгадка неминуема.

Заключеніе. Задача становится трудноразрѣшимой лишь въ томъ случаѣ, если ключъ уложился въ текстѣ ничтожное число разъ; а это бываетъ или тогда, когда текстъ очень маленькій, или когда ключъ непомѣрно большой — изъ множества буквъ. Обыкновенно употребляемые ключи колеблются между 10 и 25 буквами, а при такихъ размѣрахъ даже крошечное письмо можетъ быть разобрано. Съ длиннымъ ключомъ притомъ очень хлопотливо управляться. Необходимо также для *а* взять условно другое число взамѣнъ предательской единицы; также для *б*, *в*. Можно также замѣнить обычный порядокъ въ алфавитѣ условнымъ; практически это можно выполнить, воспользовавшись ключомъ единозначнаго парнаго шифра (см. глав. II).

ж е л ѣ з н ы й ш п и ц ъ д о м а
б в г і к р с т у ф х ч щ ь э ю я

Порядокъ буквъ надо считать вверху — слѣва направо, внизу — справа налѣво. (Ср. еще гл. XVII).

Но такое усовершенствованіе, вообще цѣлесообразное, усложняетъ, однако, шифръ и дѣлаетъ его менѣе удобнымъ для пользованія.

Но наиболѣе практичнымъ и простымъ улучшеніемъ является система, описанная въ слѣдующей главѣ.

Во всякомъ случаѣ Гамбеттовскаго шифра въ обыкновенномъ его видѣ никоимъ образомъ нельзя рекомендовать; это одна изъ самыхъ неудачныхъ системъ.

Глава IX.

СОКРАЩЕННЫЙ ГАМБЕТТОВСКІЙ ШИФРЪ.

Измѣненіе, дѣлаемое здѣсь, кажется на первый взглядъ маловажнымъ. Суммы, получающіяся отъ сложенія числовыхъ выраженій буквъ текста и ключа, превосходящія 30, уменьшаются на тридцать единицъ, т. е. вмѣсто 31 пишутъ 1, вмѣсто 38—8; вмѣсто 47—17; вмѣсто 55—25. Это — при тюремной азбукѣ, которую мы только и встрѣчали въ настоящей системѣ; если бы примѣнять полную азбуку, то слѣдовало бы скидывать не 30, а 40, ибо самый высокій знакъ при ней 68, тогда какъ при тюремной 56 (28+28).

Такимъ образомъ, число знаковъ, которыми располагаетъ система, уменьшается до 30 (1—30), вмѣсто 55 (2—56); изъ нихъ только четыре: 27, 28, 29, 30 всегда представляютъ *истинныя* суммы, остальныя могутъ быть либо дѣйствительныя, либо фиктивныя, т. е. уменьшенныя тридцатью. Напр., 17 можетъ обозначать либо 17, либо 47.

Положимъ, что требуется зашифровать по этой системѣ ключомъ: „шкурный вопросъ" такую фразу: „Намъ нуженъ наборщикъ; нѣтъ ли подходящаго?"

Для сравненія приведемъ параллельно эту же фразу, зашифрованную по той же тюремной азбукѣ *обыкновеннымъ* гамбеттовскимъ ключомъ:

Сокращ. гамбет.: 7, 11, 1, 29, 2, 3, 15, 16, 27, 16, 18, 28, 3, 19, 19, 29, 29, 19,
Обыкн. гамбет.: 37, „ 31, „ 32, 33, „ „ „ „ „ „ 33, 49, „ „ „ „
Сокращ. гамбет. (продолженіе): 14, 20, 12, 29, 29, 21, 5, 1, 29, 8, 14, 17, 17, 10.
Обыкн. гамбет. „ 44, „ „ „ „ „ 35, 31, „ 38, 44, „ „ 40.

Можетъ показаться, что такое уменьшеніе дѣйствительныхъ суммъ поставитъ получателя при чтеніи въ затрудненіе, ибо онъ не будетъ знать, какъ понимать; напр., 17—какъ таковое ли число или какъ 47. Но на самомъ дѣлѣ никакого сомнѣнія никогда не можетъ быть, ибо соотвѣтственная буква ключа даетъ готовый отвѣтъ на вопросъ. Если она меньше даннаго числа текста, то послѣднее — истинная сумма; если больше, то сумма тридцатью больше. Такъ, напр., въ вышеприведенномъ образчикѣ первое число—7; первая же буква ключа—*ш* („шкурный"...) выражается числомъ 24, слѣдовательно, истинная сумма не 7, а 37. Зато второе число 11 надо принять за настоящее, такъ какъ вторая буква ключа—*к*=10.

Особенности системы. Описанное небольшое упрощеніе на поверхностный взглядъ могло бы даже облегчить задачу раскрытія, такъ какъ число знаковъ почти вдвое сокращается. Между тѣмъ на самомъ дѣлѣ это есть громадное улучшеніе, дѣлающее совершенно недѣйствительными тѣ пріемы разгадки, которые оказались столь цѣлесообразными въ предыдущей главѣ. Шаткость, перемѣнчивый характеръ каждаго знака, свойственные гамбеттовскому шифру, здѣсь усугубляются. Первое число, напр., нашего образца 7 не только могло получиться разнообразнымъ способомъ (1+6, 2+5, 3+4, и т. д.), но оно въ дѣйствительности, быть можетъ, вовсе не 7, а 37, которое, конечно, могло получиться еще изъ большаго числа комбинацій слагаемыхъ. Исчезаетъ, такимъ образомъ, единственный прочный базисъ, который состоялъ въ томъ, что малыя числа обозначали маленькія суммы, а большія—крупныя. Между тѣмъ разгадка вся и основывалась на минимумахъ и максимумахъ. Совершенно безполезно будетъ изобразить текстъ въ видѣ кривой, ибо подъ минимальными числами 1, 2, 3, быть можетъ, скрываются 31, 32, 33; равнымъ образомъ максимальныя числа 28, 29, 30 не всегда являются наибольшими суммами. Мы не можемъ, слѣдовательно, получить прежнимъ путемъ длину ключа. Но если бы мы и знали даже это важное обстоятельство, или просто шли ощупью, беря поочередно одно число за другимъ, то и тогда мы были бы далеки отъ рѣшенія при помощи стараго метода, ибо онъ опять таки основывался на сопоставленіи минимумовъ и максимумовъ каждаго столбца таблицы № 36. — Въ смыслѣ удобства примѣненія этотъ шифръ нисколько не уступаетъ предыдущему шифру.

Задача. 28, 22, 8, 17, 19, 1, 9, 28, 9, 27, 4. 14, 29, 21. 24, 23, 10, 19, 30, 17' 22, 16, 1, 27, 17, 10, 29, 20, 2, 8. 23, 6, 29, 18, 25, 29, 12, 14, 28, 2, 5, 12, 8, 22' 12, 7, 10, 13, 7, 27. 19, 11, 14, 23, 9, 30, 13, 19, 28, 7, 24, 2, 8, 24, 2, 8, 24. 13, 1' 19, 12, 21, 29, 15, 6, 28, 2, 7, 28, 20, 24, 27, 1, 4. 18, 1. 11, 6, 26, 22, 23, 17, 23, 10, 22, 9, 11. 22, 11, 12, 11, 23. 4, 11, 29, 3, 30. 24, 9, 26, 30, 27, 25, 6, 16, 10, 19, 25, 10, 22, 26, 15, 18, 12, 27, 21, 20, 30, 19, 5, 23, 27, 15, 13, 21, 27, 30, 21, 7, 29, 17, 9, 11, 27, 1, 30, 27, 1, 4, 12, 17, 16, 10, 9, 27, 15, 26, 29, 28, 4, 27, 23, 7, 28, 8, 26, 27, 7, 8, 23, 4, 6, 4, 24, 3, 24, 29, 23, 20, 27. 2, 11, 29, 15, 8, 1, 4, 24, 28, 16, 28, 30, 21, 19, 28, 19, 5, 17, 6, 24, 4, 15, 3, 23, 29, 6, 22, 28, 5, 24, 21, 12, 24, 27, 25, 19, 28, 15, 1, 10, 22. 7, 13, 25, 24, 14, 9, 9, 2, 20, 30, 19, 11, 29, 7, 1, 9, 12.

Распознаваніе системы. Діагносцировать систему можно съ перваго же взгляда. Число знаковъ только 30, отъ 1 до 30. Это сейчасъ же указываетъ, что имѣемъ дѣло съ разбираемой формой.

Въ VII главѣ, говоря о простомъ квадратномъ шифрѣ, мы указывали, что когда таблица превосходитъ размѣрами 10×10 клѣтокъ, то дробные знаки $^1/_{11}$, $^{15}/_{16}$ и т. д. можно писать сплошнымъ рядомъ чиселъ, вставляя лишь передъ однозначнымъ числителемъ или знаменателемъ по нулю. Тоже самое, какъ мы видѣли въ предыдущей главѣ, можно продѣлать и съ гамбеттовскимъ шифромъ. Какъ же ихъ отличить? Это совсѣмъ не трудно. При квадратномъ шифрѣ каждая буква выражается четырехзначнымъ числомъ (по двѣ цифры на числителя и знаменателя), слѣдовательно, общее число цифръ будетъ кратное 4, а при гамбеттовскомъ лишь четное. Во вторыхъ, въ послѣднемъ случаѣ двухзначныя числа будутъ отъ 01 до 30, съ преобладаніемъ высокихъ, между тѣмъ какъ въ квадратномъ таблица 30×30 вообще невѣроятна, а преобладаніе будетъ во всякомъ случаѣ за малыми числами, ибо всегда

забираютъ болѣе близкіе знаки. Однимъ словомъ, отличіе будетъ сдѣлано быстро и безошибочно.

Раскрытіе шифра. Необходимо и тутъ прежде всего добраться до длины ключа, т. е. до числа буквъ въ немъ. Вернемся для этого къ таблицѣ № 36 предыдущей главы. Какъ ни мало тамъ буквъ, а между тѣмъ въ каждомъ вертикальномъ столбцѣ этой таблицы нѣкоторыя числа повторяются по 2 и даже по 3 раза. Напр., въ I столбцѣ два раза 9, во II—3 раза 7; въ IV—по два раза 14 и 34 и т. д. Отчего это происходитъ? Очевидно отъ того, что болѣе употребительныя буквы попадаютъ въ столбецъ не однажды, и, будучи сложены съ одной и той же буквой ключа, даютъ одинаковыя суммы. Напримѣръ, въ IV столбецъ по два раза попали буквы *а* (1) и *у* (21) и по сложеніи съ буквой л (13) ключа получилось въ результатѣ два раза 14 и 34. Очевидно, что разстояніе отъ перваго 14 до второго 14 въ IV столбцѣ равно цѣлому числу горизонтальныхъ рядовъ (см. табл. № 36), иными словами, число буквъ отъ одного 14 до другого 14 обязательно *кратно* длинѣ ключа, т. е. дѣлится на него. Тоже самое относится и до всякой группы одинаковыхъ чиселъ, повторяющихся въ вертикальныхъ столбцахъ. Конечно, число 14 встрѣчается спорадически и въ другихъ столбцахъ, и разстояніе до нихъ отъ тождественныхъ чиселъ IV столбца уже не будетъ кратное длины ключа.

Очевидно, что тоже самое цѣликомъ приложимо и къ „сокращенному гамбеттовскому шифру", ибо въ *этомъ* отношеніи между ними нѣтъ разницы.

Итакъ, группировка однихъ и тѣхъ же знаковъ въ текстѣ въ скрытомъ видѣ содержитъ разрѣшеніе вопроса о длинѣ ключа. Повторяющихся знаковъ, конечно, много въ текстѣ, ибо тридцатью знаками выражаются 238 буквъ; они отстоятъ другъ отъ друга на самыхъ различныхъ разстояніяхъ—отъ одной буквы до 230. Только нѣкоторыя изъ этихъ разстояній кратны длины ключа, остальныя къ дѣлу не относятся. Какъ ихъ выдѣлить изъ массы ненужныхъ? Если собрать *всѣ* разности, то благодаря превалированію среди нихъ специфическаго ряда, онъ сейчасъ же обнаружится.

Поступаемъ такъ. Пронумеруемъ по порядку всѣ буквы „задачи" отъ первой до 238-й. Начнемъ со знака „1" и выпишемъ всѣ мѣста, занимаемыя имъ въ текстѣ. Таковыхъ окажется десять: 6, 23, 69, 79, 82, 145, 148, 186, 219, 236. Если вычесть 1-ое число (6) изъ остальныхъ, то узнаемъ разстоянія отъ перваго до каждаго изъ нихъ. Если въ полученныхъ такимъ образомъ разностяхъ вычесть первую изъ всѣхъ послѣдующихъ, то узнаемъ разстоянія отъ 2-го числа (23) до всѣхъ остальныхъ. Такъ мы поступаемъ до послѣдняго. Помѣщаемъ здѣсь для примѣра способъ полученія разностей для знаковъ „1" и „2".

Знакъ „1". *Таблица № 37.*

Мѣста въ текстѣ: 6, 23, 69, 79, 82, 145, 148, 186, 219, 236

Разности:

17, 63, 73, 76, 139, 142, 180, 213, 230
46, 56, 61, 122, 125, 163, 196, 213
10, 15, 76, 79, 117, 150, 167
5, 66, 69, 107, 140, 157
51, 64, 102, 135, 145
13, 51, 84, 94
38, 71, 81
33, 43
10

Знакъ „2". *Таблица № 38.*

Мѣста въ текстѣ: 29, 40, 62, 65, 77, 181, 229

Разности:

11, 33, 36, 48, 152, 200
22, 25, 37, 141, 189
3, 15, 119, 167
12, 116, 164
104, 152
48

Обслѣдуя такимъ же образомъ всѣ остальные знаки вплоть до послѣдняго „30“, мы получаемъ громадное число разностей, которыя мы суммируемъ на особой таблицѣ (см. таблицу № 39). Она содержитъ 220 клѣтокъ; слѣва числа обозначаютъ десятки и сотни, верхній горизонтальный рядъ—единицы. Такимъ образомъ, напр., 6-ая клѣтка 14-го ряда соотвѣтствуетъ разности 145. Числа, стоящія въ клѣткахъ, выражаютъ повторяемость разности. Въ упомянутой клѣткѣ 145—стоитъ 0(тире), т. е. эта разность не встрѣтилась ни одного раза; разность 31 встрѣчается 7 разъ, и т. д.

Для нашей цѣли совершенно достаточно ограничиться самыми частыми разностями, такъ какъ въ нихъ то скорѣе всего скрывается таинственное число, выражающее длину періода. Выпишемъ ихъ:

Повторяется

16	разъ:	*85.*
13	„	26.
12	„	14, 3.
11	„	9, *17.*
10	„	11, *34.*
9	„	5, 12, 13, 16, 22, *51.*
8	„	2, 25, 30, 37, 38, 46, 49, 57, 117, *119, 170.*

На самой верхушкѣ стоитъ 85, т. е. 5×17. Далѣе находимъ: 17, 34 (2×17), 51 (3×17), 119 (7×17), 170 (10×17). Ничего подобнаго мы не находимъ среди другихъ чиселъ. Ясно, что именно эти выписанныя нами числа, которыя всѣ кратны 17, скрываютъ въ себѣ длину періода; ясно также, что это и есть 17, что въ ключѣ 17 буквъ. Для провѣрки выпишемъ всѣ остальныя числа, кратныя 17, въ предѣлахъ нашей таблицы, и посмотримъ ихъ повторяемость:

17—одиннадцать	разъ	85—шестнадцать	разъ	153—пять	разъ	221—0	разъ
34—десять	„	102—шесть	„	170—восемь	„		
51—девять	„	119—восемь	„	187—три	„		
68—семь	„	136—шесть	„	204—два	„		

Таблица № 39.

	0	1	2	3	4	5	6	7	8	9
0		1	8	12	5	9	6	4	7	11
1	3	10	9	9	12	4	9	11	4	7
2	5	4	9	6	5	8	13	5	5	5
3	8	7	5	4	10	2	5	8	8	7
4	5	4	6	5	6	4	8	7	6	8
5	2	9	4	5	4	6	3	8	5	6
6	5	2	7	3	3	6	6	5	7	7
7	2	2	5	6	7	4	7	5	4	7
8	3	3	—	6	5	16	4	7	4	6
9	6	2	3	2	2	2	7	6	2	6
10	3	2	6	7	3	4	3	2	2	6
11	4	4	6	4	3	4	4	8	4	8
12	3	6	3	4	5	1	2	3	4	6
13	1	4	7	5	5	1	6	1	4	3
14	2	3	3	4	7	—	6	4	3	3
15	2	1	2	5	2	4	1	2	2	4
16	3	3	2	2	4	—	2	4	—	3
17	8	2	4	3	1	4	2	2	3	1
18	1	—	2	2	1	3	3	3	2	1
19	1	3	1	2	1	3	—	3	2	1
20	1	1	1	—	2	—	1	1	1	1
21	1	2	—	1	—	1	2	1	2	—
22	—	—	—	—	1	—	—	1	—	—

Таблица № 40.

	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}
	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV	XVI	XVII
А	28	22	8	17	19	1	9	28	9	27	4	14	29	21	24	23	10
Б	19	30	17	22	16	1	27	17	10	29	20	2	8	23	6	29	18
В	25	29	12	14	28	2	5	12	8	22	12	7	10	13	7	27	19
Г	11	14	23	9	30	13	19	28	7	24	2	8	24	13	1	19	12
Д	21	29	15	6	28	2	7	28	20	24	27	1	4	18	1	11	6
Е	26	22	23	17	23	10	22	9	11	22	11	12	11	23	4	11	29
Ж	3	30	24	9	26	30	27	25	6	16	10	19	25	10	22	26	15
З	18	12	27	21	20	30	19	5	23	27	15	13	21	27	30	21	7
И	26	17	9	11	27	1	30	27	1	4	12	17	16	10	9	27	15
І	26	29	28	4	27	23	7	28	8	26	27	7	8	23	4	6	4
Й	24	3	24	29	23	20	27	2	11	29	15	8	1	4	24	28	19
К	28	30	21	19	28	19	5	17	6	24	4	15	3	23	29	6	22
Л	28	5	24	21	12	24	27	25	19	28	15	1	10	22	7	13	25
М	24	14	9	9	2	20	30	19	11	29	7	1	9	12			

Для полученія того же результата можно было даже и не опредѣлить разностей для *всѣхъ* знаковъ; достаточно было бы и нѣсколькихъ.

Зная уже такой важный элементъ, какъ длина ключа, раздѣлимъ нашу „задачу“ на грани по 17 буквъ въ каждой и подпишемъ ихъ одну подъ другой совершенно такъ же, какъ на таблицѣ № 36. (См. табл. № 40).

Римскія цифры означаютъ номера вертикальныхъ столбцовъ, буквы X_1, X_2, X_3 и т. д.—неизвѣстныя буквы ключа, соотвѣтствующія столбцамъ: заглавныя буквы слѣва — горизонтальные ряды, каковыхъ имѣется 14. На тщательномъ анализѣ вертикальныхъ столбцовъ основывается рѣшеніе задачи.

Мы знаемъ, что въ азбукѣ центральный отдѣлъ заключаетъ сплошной рядъ частыхъ буквъ (см. табл. № 5); при тюремной азбукѣ, которая примѣнена въ настоящемъ случаѣ, этотъ отдѣлъ обнимаетъ буквы и, к, л, м, н, о, п, р, с, т, у, за которыми начинается отдѣлъ рѣдкихъ буквъ. Изъ каждыхъ 10 буквъ текста на центральный отдѣлъ приходится въ среднемъ *6* буквъ. Очевидно, то же относится и ко всякому вертикальному столбцу таблицы № 40. Изъ каждыхъ 14 буквъ столбца—8,4 придется въ среднемъ на центральный отдѣлъ азбуки. Но такъ какъ числовыя обозначенія буквъ на протяженіи столбца измѣнены равномѣрно — на букву ключа, то такое преобладаніе центральнаго отдѣла должно открыто выступить и послужить базисомъ для раскрытія.

Размѣстимъ наши 17 столбцовъ для наглядности графически (см. табл. № 41)*. Они расположены въ видѣ 17 горизонтальныхъ рядовъ, пронумерованныхъ римскими цифрами. Справа отъ послѣднихъ стоятъ буквы X_1, X_2, X_3, X_4..., соотвѣтствующія неизвѣстнымъ буквамъ ключа. Сверху идетъ нумерація отъ 1 до 30, соотвѣтственно числу *знаковъ* разбираемой системы. Подъ соотвѣтственными числами разнесены въ клѣткахъ горизонтальныхъ рядовъ знаки каждаго столбца — въ формѣ черточки. Двойная, тройная черточка означаетъ, что соотвѣтственное число повторяется въ столбцѣ 2, 3 раза.

Возьмемъ для удобства изложенія какой-нибудь изъ болѣе типическихъ рядовъ, напримѣръ, V. Наибольшее сгущеніе знаковъ мы замѣчаемъ въ области 23-32(2), изъ чего заключаемъ, что это и есть центральный отдѣлъ. Въ ней срединный узелъ въ клѣткѣ 28, гдѣ сгущены три черточки, и потому здѣсь, вѣроятно, буква *о*. Провѣримъ. Буква *о* занимаетъ въ тюремной азбукѣ 14-ое мѣсто (см. глав. I), слѣдовательно, соотвѣтственная буква ключа—X_5 составляетъ 28—14, т. е. 14; если $X_5=14$, то буква *е* выразится числомъ *20*; въ ряду таковое, дѣйствительно, имѣется; буква и=23 (имѣется), т=2 (имѣется), н=27 (дважды) и т. д. Числа такъ совпадаютъ съ наиболѣе употребительными буквами, что наше предположеніе превращается въ увѣренность. Итакъ, $X_5=14=o$.

Для разгадки вовсе нѣтъ необходимости проанализировать такимъ образомъ *всѣ* ряды, хотя болѣе половины ихъ дастъ совершенно ясные, стоящіе внѣ сомнѣнія результаты. Мы ограничимся, поэтому, двумя ближайшими къ изслѣдованному выше: рядами IV и VI. Въ ряду IV центральный отдѣлъ скрывается между 14 и 22. Для буквы *о* умѣстнѣе взять 17 (лежитъ въ серединѣ и повторено дважды); тогда $X_4=3$. Провѣряемъ: а=4 (есть); е=9 (трижды); т=21 (дважды); также есть для *в*, *л*, *р*, *у*. Итакъ, $X_4=3=в$.

Въ ряду VI центральный отдѣлъ имѣетъ свое мѣстопребываніе около 30-32(2). Если *о*=31(1), то $X_6=17$. Провѣряемъ: в=20 (дважды); е=23 (есть); н=30 (дважды); п=2 (дважды); ч=10; ы=13. Итакъ, $X_6=с$.

Мы добыли уже три рядомъ стоящія буквы ключа, недалеко отъ начала его, образующія вмѣстѣ слогъ *вос*. Провѣряемъ истинность, поставивъ ихъ на таблицѣ 40 въ IV-VI вертикальные столбцы. Получаются такія сочетанія:

А=...одо..	Г=...еры..	Ж=...емн..	І=...ане..	Л=...тяж..
Б=...убо..	Д=...воп..	З=...тен..	Й=...ыив..	М=...етв..
В=...лоп..	Е=...онч..	И=...зно..	К=...роб..	

Мы видимъ, во-первыхъ, что всѣ звуковыя сочетанія совершенно правдоподобны, натуральны. Во-вторыхъ, мы получаемъ возможность сдѣлать дальнѣйшіе шаги. Въ ряду „Л“—слогъ *тяж*... непремѣнно предполагаетъ дальше букву *е* (тяжесть, тяже-

*) См. въ концѣ книги.

лый). Это дастъ намъ для X_7 значеніе 21=х, ибо въ ряду „Л“ предполагаемой буквѣ *е* соотвѣтствуетъ число 27. Мы можемъ, слѣдовательно, продолжить наши слоги:

А=...одот...	Е=...оича...	Й=...ыиве...
Б=...убое...	Ж=...емне...	К=...робо...
В=...лопо...	З=...теня...	Л=...тяже...
Г=...ерыя...	И=...зной...	М=...етви...
Д=...вопр...	І=...анер...	

Тутъ можно уже заподозрить много словъ, напр., въ Г — серыя (сѣрыя), въ И—знойный, въ М—вѣтви и т. д. Находимъ, такимъ образомъ: $X_8=14=o$; $X_3=6=e$. Подставивъ и эти значенія, мы подвигаемся далѣе уже рѣшительно безъ всякихъ затрудненій. Напр., Б дастъ намъ: „...лубое“ = голубое. Найденная часть ключа составитъ „превосхо...“.

Мы не будемъ утомлять читателя дальнѣйшимъ разборомъ. Станемъ ли мы анализировать остальные ряды таблицы 41, или продолжать дальше подстановку открываемыхъ буквъ ключа въ таблицу 40, или ускорять дѣло, отгадывая смыслъ самого ключа, — результатъ будетъ одинъ: задача будетъ безпрепятственно рѣшена. Ключъ окажется „превосходная читка“, а текстъ такой:

„Небо, до того времени голубое, вдруг потускнело. Появились густыя, серыя облака. Они лениво проплывали над лесной чащей, которая то темнела въ их багровых тенях, то опят млела в знойных лучах солнца. Неровныи, порывистыи ветерокъ тщетно пробовал всколыхнут тяжело повиснувшия ветви деревев“.

Заключеніе. Итакъ, и эта система не годится. Разумѣется, если взять очень длинный ключъ и очень малый текстъ, то періодичность проявится такъ слабо, что раскрытіе можетъ оказаться невозможнымъ; но большіе ключи мало удобны, а размѣръ текста зависитъ отъ обстоятельствъ; тѣмъ болѣе, что нѣсколько малыхъ записей равносильны одному большому тексту*). Приходится искать лучшей системы.

Глава X.

ЗАМАСКИРОВАННЫЙ ГАМБЕТТОВСКІЙ ШИФРЪ.

(„Наполеоновскій“).

Курьезная система эта, носящая почему-то громкое названіе „наполеоновской“, какъ существенную часть свою, предполагаетъ большую квадратную таблицу изъ 28×28 клѣтокъ (табл. № 42). Въ первомъ горизонтальномъ и лѣвомъ вертикальномъ рядахъ пишемъ непрерывный послѣдовательный рядъ чиселъ отъ 1 до 28 (по числу буквъ тюремной азбуки). Затѣмъ выполняемъ по порядку всѣ горизонтальныя строки, начиная отъ крайняго лѣваго числа: всякій разъ, какъ доходимъ до 28, мы въ слѣдующей клѣткѣ начинаемъ опять съ единицы. Наконецъ, выше перваго ряда чиселъ и лѣвѣе перваго столбца выписываемъ тюремную азбуку. Такова таблица — необходимая принадлежность „наполеоновскаго“ шифра, одинаковая при самыхъ различныхъ ключахъ и отъ послѣднихъ независимая.

Ключомъ же служитъ условленная фраза или слово.

Пусть ключомъ будетъ „шкурныи вопрос“, и требуется зашифровать фразу: „Намъ нуженъ наборщикъ, нѣтъ ли подходящаго“. Чтобы записать первую букву *н*, отыскиваемъ тотъ горизонтальный рядъ, который начинается этой буквой (т. е. тринадцатый), а затѣмъ тотъ вертикальный столбецъ, который начинаетси первой буквой ключа — *ш* (то будетъ 24-ый). Отыскиваемъ клѣтку, стоящую на мѣстѣ скрещенія обоихъ этихъ столбцовъ — въ ней имѣется число 8, которое и пишемъ въ криптограммѣ вмѣсто буквы *н*. Такимъ же образомъ вторую букву текста — *а* слѣдуетъ

---

*) Этотъ шифръ можетъ стать совершенно неразрѣшимымъ, если взять для ключа большой отрывокъ изъ книги или стихотворенія, но тогда онъ перестаетъ быть періодическимъ (подробнѣе см. глав. XIX).

искать на мѣстѣ скрещенія 1-го горзонтальнаго ряда съ десятымъ вертикальнымъ (столбцомъ буквы *к* ключа) — найдемъ число *10*. Приведенная для примѣра фраза зашифруется такъ: 8, 10, 2, 28, 3, 4, 14, 15, 26, 15, 17, 27, 4, 20, 18, 28, 28, 18, 15, 19, 11, 28, 28, 20, 6, 2, 28, 9, 15, 16, 16, 11.

Особенности системы. Система располагаетъ всего 28 знаками: отъ 1 до 28, и принадлежитъ къ разряду перемѣннозначныхъ; напр., число 28, повторяющееся въ нашей примѣрной коротенькой фразѣ 6 разъ, обозначаетъ слѣдующія буквы: н, к, н, п, о, д. По внѣшнему виду криптограммы система напоминаетъ гамбеттовскую, въ особенности сокращенную, но она гораздо менѣе удобна для примѣненія, чѣмъ послѣдняя: составленіе таблицы отнимаетъ добрые пол-часа, да и пользованіе ею, благодаря размѣрамъ, мало удобно. Посмотримъ теперь, насколько этотъ практическій недостатокъ выкупается надежностью и неприступностью шифра.

Распознаваніе системы. Какъ мы уже указали, она по внѣшнему своему виду вполнѣ напоминаетъ „сокращенную гамбеттовскую", описанную въ предыдущей главѣ. Однако, ихъ нетрудно отличить другъ отъ друга. Тутъ число знаковъ отъ 1 до 28; тамъ—отъ 1 до 30. Поэтому въ наполеоновскомъ шифрѣ совершенно отсутствуютъ знаки 29 и 30, что сразу его и выдаетъ.

Раскрытіе шифра. Если вдуматься въ сущность разбираемой системы, то не много потребуется сообразительности, чтобы понять, что тутъ скрывается какое то крупное недоразумѣніе, курьезный самообманъ. Посмотримъ, напримѣръ, какъ получился у насъ *второй* знакъ нашего образчика — *10*, выражающій букву *а* текста и

Таблица № 42.

	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ы	ю	я
а	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
б	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1
в	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2
г	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3
д	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4
е	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5
ж	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6
з	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7
и	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8
к	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9
л	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10
м	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11
н	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12
о	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13
п	15	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14
р	16	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
с	17	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
т	18	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
у	19	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ф	20	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
х	21	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ц	22	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
ч	23	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
ш	24	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
щ	25	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
ы	26	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
ю	27	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
я	28	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

соотвѣтствующій второй буквѣ ключа *к*. Мы разыскали сперва *первый* горизонтальный рядъ (ибо *а* по мѣсту своему въ алфавитѣ=1). Затѣмъ 10-ый вертикальный столбецъ (ибо к=10), и потомъ взяли число 10, стоящее на скрещеніи. Четвертая буква текста *н*(=13) вмѣстѣ съ четвертой буквой ключа *р* (=16) дало 28, т. е. сумму обоихъ чиселъ, уменьшенную на единицу. Первая буква текста (н=13) вмѣстѣ съ первой буквой ключа (ш=24) должно было дать 36 (т. е. сумму безъ одного), но такъ какъ числа въ рядахъ идутъ только до 28, а дальше начинается опять съ единицы, то понятно, что вмѣсто 36 оказалось въ клѣткѣ 8 (36—28). Однимъ словомъ, при этой системѣ знаки получаются совершенно просто: отъ сложенія буквъ текста и буквъ ключа. Есть только двѣ особенности, отличающія ее отъ системъ, разсмотрѣнныхъ въ предыдущихъ двухъ главахъ; во 1-ыхъ, записывается не вся сумма, а уменьшенная на единицу, а во вторыхъ, изъ чиселъ большихъ 28, вычитается 28: вмѣсто 40—пишутъ 12, вмѣсто 51—23 и т. д. Чтобы вполнѣ удостовѣриться въ этомъ, сравнимъ зашифрованный здѣсь образчикъ съ тѣмъ же образчикомъ, записаннымъ по тому же ключу въ предыдущихъ главахъ (гл. VIII и IX):

(I) Простой гамбет.: 37, 11, 31, 29, 32, 33, 15, 16, 27, 16, 18, 28, 33, 49, 19,
(II) Сокращ. гамбет.: 7, 11, 1, 29, 2, 3, 15, 16, 27, 16, 18, 28, 3, 19, 19,
(III) Наполеоновскій: 8, 10, 2, 28, 3, 4, 14, 15, 26, 15, 17, 27, 4, 20, 18.
(I) 29, 29, 19, 44, 20, 12, 29, 29, 21, 35, 31, 29, 38, 44, 17, 17, 40.
(II) 29, 29, 19, 14, 20, 12, 29, 29, 21, 5, 1, 29, 8, 14, 17, 17, 10.
(III) 28, 28, 18, 15, 19, 11, 28, 28, 20, 6, 2, 28, 9, 15, 16, 16, 11.

Итакъ, чтобы шифровать по этой системѣ, надо складывать буквы текста и буквы ключа и уменьшать на единицу; если получится число меньшее 28, то такъ и записывать, если же большее, то вычитать изъ него 28. Но въ такомъ случаѣ зачѣмъ же намъ громоздкая, отнимающая массу времени для составленія и даже мало удобная для пользованія табл. 41? Она совершенно ненужна. Невольно вспоминается разсказъ про солдата, который варилъ супъ изъ „бороньяго зуба"; но тотъ сознательно дурачилъ свою жадную хозяйку, а здѣсь революціонеръ съ наивной вѣрой обманываетъ самого себя.

Разумѣется, ни терпѣливое составленіе ненужной таблицы, ни „усовершенствованіе" по существу, заключающееся въ томъ, что число знаковъ тутъ не 30, а 28, нисколько не дѣлаетъ „наполеоновскій" шифръ надежнѣе „сокращеннаго гамбеттовскаго". Сюда приложимы тѣ же методы раскрытія какъ длины ключа, такъ и самого содержанія его. Поэтому брать „задачу" и анализировать ее значитъ повторять все сказанное въ предыдущей главѣ.

Заключеніе. Наполеонъ когда-то сказалъ, что отъ великаго до смѣшного одинъ шагъ. Курьезно, что носящій его великое имя шифръ, оказывается смѣшнымъ фарсомъ, водевилемъ съ переодѣваніемъ. А между тѣмъ онъ кое-гдѣ у насъ употребляется *).

Глава XI.

РАЗНОСТНЫЙ ГАМБЕТТОВСКІЙ ШИФРЪ

съ двойнымъ періодомъ.

Раздѣльныя періодическія системы, которыя мы до сихъ поръ разсматривали, основывались на *сложеніи* буквъ текста и ключа. Но, разумѣется, вмѣсто того, чтобы складывать ихъ, можно было бы съ успѣхомъ производить и *вычитаніе*. Съ такими „разностными" гамбеттовскими шифрами мы, однако, на практикѣ не встрѣчались, и такъ какъ они къ тому же не представляютъ ничего особеннаго ни со стороны техники, ни со стороны раскрытія, то мы не считаемъ нужнымъ спеціально на нихъ

*) Какъ курьезъ отмѣтимъ, что въ 1902 г. въ кіевской тюрьмѣ этотъ шифръ былъ *рекомендованъ*, какъ *безусловно надежный*, совершенно недоступный раскрытію.

останавливаться. Мы ограничимся описаніемъ одной усложненной формы разностнаго періодическаго шифра, съ которою мы встрѣчались въ революціонной практикѣ.

Возьмемъ достаточно знакомый уже намъ ключъ: „шкурный вопросъ“ и фразу: „намъ нуженъ наборщикъ...“.

Первая буква ключа *ш* (=24 по тюремной азбукѣ) больше первой буквы текста *н* (=13) на 11. Это мы выразимъ такимъ образомъ: 1—11. Въ этомъ двучленѣ единица обозначаетъ *первую* букву текста, а „—11“, что она *меньше* 1-ой буквы ключа на одиннадцать единицъ.

Вторая буква ключа *к* (=10) больше *второй* буквы текста *а* (=1) на 9, что мы выразимъ такъ: 2—9.

Точно такъ же третья буква текста изобразится въ видѣ 3—7; четвертая 4—3.

Пятая буква ключа *н* (=13) *меньше* соотвѣтствующей буквы текста *у* (=19), поэтому послѣдняя изобразится въ формѣ суммы: 5+6.

Поступая такимъ же образомъ дальше, возвращаясь снова къ началу ключа послѣ использованія его послѣдней буквы, мы найдемъ для взятой въ качествѣ образчика фразы слѣдующее выраженіе: 1—11, 2—9, 3—7, 4—3, 5+6, 6—19, 7—3, 8+10, 9—13, 10—13, 11+9, 12—5, 13—7...

Этимъ, однако, дѣло не кончается. На сцену выступаетъ второй періодъ, представляемый обыновенно короткимъ числомъ, напр., 795. Назовемъ это послѣднее „вторичнымъ періодомъ“ или „числовымъ ключомъ“. Три цифры его 7, 9, 5 будемъ послѣдовательно прибавлять къ каждому члену нашихъ двучленовъ:

Первичный текстъ . . .	1—11;	2— 9;	3— 7;	4— 3;	5+ 6;...
+					
Числовой ключъ	7, 9, 5;	7, 9, 5;	7, 9, 5;	7, 9, 5;	7,...
Окончательный текстъ . .	8—20;	7—16;	12—12;	11—12;	10+13;...

Особенности системы. Криптограмма имѣетъ весьма своеобразный видъ; каждая буква выражается двучленной формулой или биномомъ (суммой или разностью); вторые члены биномовъ колеблются въ не очень широкихъ предѣлахъ, ибо въ основѣ ихъ лежитъ разница между двумя буквами; первые же члены постепенно возрастаютъ, хотя медленно и съ колебаніями: они представляютъ въ сущности измѣненную числовымъ ключомъ нумерацію буквъ текста. Такимъ образомъ, хотя и возможно повтореніе одинаковыхъ знаковъ, т. е. тождественныхъ биномовъ, но, вообще, какъ правило, знаковъ столько же, сколько буквъ въ текстѣ. Обстоятельство это придаетъ шифру весьма грозный, непобѣдимый видъ, тѣмъ болѣе, что въ основѣ лежатъ *два* періода. Зато нельзя отрицать, что съ точки зрѣнія примѣненія шифръ представляетъ нѣчто до крайности тяжеловѣсное: приходится и при шифровкѣ, и при чтеніи производить цѣлый рядъ манипуляцій, при которыхъ легко спутаться и надѣлать ошибокъ; въ этомъ отношеніи ему принадлежитъ пальма первенства изъ всѣхъ разбираемыхъ здѣсь системъ. Къ тому же криптограмма пріобрѣтаетъ чрезвычайно растянутый видъ, ибо на каждую букву приходится не двѣ и даже не 4 цифры, а цѣлый биномъ.

Задача. 3+9; 7+7; 12—12; 7+8; 12—32; 8+4; 12+16; 17+6; 12+8; 17+16; 13—6; 17+11; 22—7; 17—21; 22—16; 18+7; 22—8; 27+5; 22+12; 27+14; 23+10; 27—16; 32—16; 27—12; 32—15; 28—8; 32+22; 37+14; 32—7; 37+12; 33+6; 37—17; 42+8; 37+15; 42+9; 38+13; 42—8; 47+7; 42+7; 47+14; 43—17; 47+22; 52—8; 47—6; 52+19; 48+5; 52+18; 57—10; 52+13; 57—20; 53+8; 57+24; 62+20; 57+21; 62—10; 58+13; 62+21; 67+19; 62—19; 67—20; 63+5; 67—16; 72+11; 67—11.

Кажущаяся такой длиной криптограмма содержитъ всего на всего 64 буквы.

Распознаваніе системы. Никакимъ сомнѣніямъ тутъ не можетъ быть мѣста: діагнозъ ставится съ перваго взгляда.

Раскрытіе шифра. Прежде всего необходимо опредѣлить „вторичный періодъ“, т. е. „числовой ключъ“. Задача оказывается необыкновенно простой.

Вспомнимъ, что первые члены биномовъ представляютъ простую нумерацію: 1, 2, 3, 4, 5, 6 и т. д., лишь измѣненную отъ наложенія различныхъ цифръ „числового ключа“. Выпишемъ поэтому *первые* члены нѣсколькихъ начальныхъ биномовъ, а подъ ними ихъ естественную первоначальную нумерацію:

Первые члены биномовъ .	3,	7,	12,	7,	12,	8,	12,	17,	12,	17,	13,	17,	22,	17...
Нумерація	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14...
Разности	2,	5,	9,	3,	7,	2,	5,	9,	3,	7,	2,	5,	9,	3...

Нетрудно понять, что нижній рядъ (разности) заключаетъ въ себѣ цифры ключа, которыя были прибавлены при шифрованіи къ „нумераціи" и дали верхній рядъ. Вспомнимъ, однако, что пользуясь „числовымъ ключомъ", мы только тѣ цифры его, которыя стояли на нечетныхъ мѣстахъ (т. е. первую, третью, пятую и т. д.), прикладывали къ первымъ членамъ биномовъ, прочія же цифры его (т. е. стоявшія на четныхъ мѣстахъ) прибавлялись всегда ко вторымъ членамъ биномовъ. Слѣдовательно, найденныя нами цифры не должны быть сдвинуты до взаимнаго соприкосновенія и не составляютъ сплошь ключа, а стоятъ въ немъ на нечетныхъ мѣстахъ, и между каждыми двумя сосѣдними цифрами долженъ быть оставленъ промежутокъ для неизвѣстной цифры. Изобразивъ ее точкой, получимъ такой видъ для цифръ числового ключа: 2.5.9.3.7.2.5.9.3.7.2.5.9.3.7.2.5.9.3.7.2..

Періодичность строенія этого ряда сразу бросается въ глаза. Періодъ составляетъ десятицифирная группа *2.5.9.3.7.*, въ коей лишь половина намъ извѣстна.

Легко, однако, доказать, что періодичность можетъ съ полнѣйшимъ успѣхомъ быть сведена къ половинному количеству цифръ, т. е. къ пяти. Въ самомъ дѣлѣ, раздѣлимъ нашъ періодъ пополамъ

2.5.9 | .3.7.

и предположимъ, что вторая часть его тождественна съ первой. Ихъ взаимоположеніе окажется таковымъ:

	I	II	III	IV	V
Первая половина . .	2	.	5	.	9
Вторая „ . . .		3	.	7	.
Ключъ	2	3	5	7	9

Вторая половина десятицифирнаго періода вошла въ пары первой и никакого противорѣчія съ первымъ рядомъ не получилось:

Первый рядъ
(10 цифирный): 2 . 5 . 9 . 3 . 7 . | 2 . 5 . 9 . 3 . 7 . | ...
Второй рядъ
(5 цифирный): 2 *3* 5 *7* 9 | *2* 3 5 *7* *9* | 2 *3* 5 *7* 9 | *2* 3 5 *7* *9* | ...

Разсужденіе это показываетъ намъ, что возможны двѣ комбинаціи: 1) или „числовой ключъ" состоитъ изъ 5 цифръ (нечетнаго количества ихъ) и тогда онъ намъ цѣликомъ извѣстенъ: 23579; 2) или же онъ состоитъ изъ 10 цифръ (четнаго количества), и тогда половина ихъ намъ остается неизвѣстной. Какъ можно было бы открыть эти неизвѣстныя цифры, мы покажемъ въ концѣ главы, но пока мы должны остановиться на болѣе простомъ, болѣе вѣроятномъ и вполнѣ извѣстномъ пятицифирномъ ключѣ 23579.

Вычтя цифры этого ключа послѣдовательно изъ всѣхъ членовъ биномовъ, получимъ первоначальный текстъ:

1+6; 2+0; 3−10; 4+3; 5−23; 6+1; 7+9; 8+4; 9+3; 10+7; 11−3; 12+4; 13−5; 14−16; 15−8; 16+4; 17−1; 18+3; 19+7; 20+5; 21+7; 22−9; 23−14; 24−7; 25−6; 26−5; 27+15; 28+12; 29−2; 30+3; 31+3; 32—10; 33+6; 34+8; 35+0; 36+10; 37—1; 38+5; 39+2; 40+5; 41—14; 42+15; 43—6; 44—1; 45+10; 46+2; 47+11; 48−8; 49+8; 50−11; 51+5; 52+17; 53+18; 54+16; 55−1; 56+10; 57+14; 58+17; 59−14; 60 -11; 61+2; 62—9; 63+9; 64−6.

На очередь выдвигается теперь вопросъ объ опредѣленіи длины „первичнаго періода", т. е. „буквеннаго ключа". Методъ его опредѣленія совершенно такой же, какъ для „сокращеннаго гамбеттовскаго" шифра, но здѣсь понять его нѣсколько труднѣе.

Обратимся назадъ къ таблицѣ № 36 или № 40, гдѣ криптограммы гамбеттовскихъ системъ, по раздѣленіи на грани соотвѣтственно длинѣ ключа, расположены въ столбцы. Мы говорили уже, что въ столбцахъ обязательно и преимущественно соби-

раются повторные знаки, и что это неизбѣжно; въ столбецъ какъ ни какъ *должны* попасть одинаковыя буквы текста и, складываясь съ одной и той же буквой ключа, даютъ въ результатѣ одинаковые знаки. Вообразимъ теперь, что въ такой столбецъ попали двѣ буквы *к* (=10), при буквѣ ключа *у* (=19, т. е. на *9* больше), и положимъ, что первая буква *к* занимаетъ въ текстѣ 23-ье мѣсто, а вторая *к*—45-ое. Тогда первая буква по разбираемой системѣ изобразится въ видѣ *23—9*, а вторая: *45—9*. Въ обоихъ этихъ различныхъ биномахъ ихъ вторые члены (—9) тождественны, и причина лежитъ не въ чемъ иномъ, какъ въ тождественности буквъ, ими выражаемыхъ. Отсюда ясно, что стоитъ только проанализировать положеніе въ текстѣ *повторныхъ* вторыхъ членовъ биномовъ совершенно такимъ же образомъ, какъ мы это сдѣлали въ IX главѣ съ повторными знаками (напр., 1, 13, 28...), чтобы извлечь скрытый періодъ. Нумеровать здѣсь знаки текста не приходится, ибо они уже пронумерованы. Приведемъ для образчика опредѣленіе разностей для „—1", „+2" и „+10". (Ср. табл. №№ 37 и 38).

Таблица № 43.

Второй членъ бинома „—1".

Мѣста въ текстѣ (или что то же—первые члены биномовъ): 17, 37, 44, 55

Разности. 20, 27, 38
7, 18
11.

Второй членъ бинома „+2".

Мѣста въ текстѣ: 39, 46, 61

Разности. 7, 22
15.

Второй членъ бинома „+10".

Мѣста въ текстѣ: 36. 45, 56

Разности. 9, 20
11.

Продѣлавъ то же самое со всѣми повторными членами, которыхъ здѣсь, благодаря ничтожной величинѣ криптограммы, вообще очень мало, суммируемъ всѣ разности и наносимъ результатъ подсчета на табличку, совершенно аналогичную таблицѣ № 39 главы IX (см. таблицу № 44).

Выпишемъ самыя частыя разности:

5 разъ встрѣчаются разности 13, *18*.
3 „ „ „ 11, 15.
2 „ „ „ 1, 4, 7, *9*, 14, 20, *27*.

На вершинѣ стоятъ два числа 13 и 18, изъ нихъ только второе оказывается вѣроятнымъ, такъ какъ находитъ себѣ двѣ родственныя разности: 9 и 27. Разсматривая рядъ чиселъ 9, 18, 27, мы съ необходимостью заключаемъ, что искомая длина періода — 9, иначе говоря, буквенный ключъ состоитъ изъ девяти буквъ. Сдѣлавъ это важное пріобрѣтеніе, разобьемъ нашъ первичный текстъ на грани изъ 9 буквъ въ каждой и подпишемъ ихъ одну подъ другой, какъ мы сдѣлали на табл. №№ 36 и 40. (См. табл. № 45).

Таблица № 44.

	0	1	2	3	4	5	6	7	8	9
0	—	2	1	—	2	—	1	2	1	2
1	1	3	1	5	2	3	—	—	5	—
2	2	—	1	—	—	—	1	2	—	1
3	—	1	1	1	—	—	1	—	1	1
4	1	—	—	—	—	—	—	—	—	—
5	—	—	—	—	—	—	1	—	—	—

Къ полученной таблицѣ приложимы вполнѣ тѣ же разсужденія, которыя помогли намъ разобраться въ таблицѣ № 36 простого гамбеттовскаго шифра. Возьмемъ I-й столбецъ; неизвѣстная буква ключа, ему соотвѣтствующая,—X_1; каждый биномъ его

Таблица № 45.

X_1 I	X_2 II	X_3 III	X_4 IV	X_5 V	X_6 VI	X_7 VII	X_8 VIII	X_9 IX
1+ 6	2+ 0	3−10	4+ 3	5−23	6+ 1	7+ 9	8+ 4	9+ 3
10+ 7	11− 3	12+ 4	13− 5	14−16	15− 8	16+ 4	17− 1	18+ 3
19+ 7	20+ 5	21+ 7	22− 9	23−14	24− 7	25− 6	26− 5	27+15
28+12	29− 2	30+ 3	31+ 3	32−10	33+ 6	34+ 8	35+ 0	36+10
37− 1	38+ 5	39+ 2	40+ 5	41−14	42+15	43− 6	44− 1	45+10
46+ 2	47+11	48− 8	49+ 8	50−11	51+ 5	52+17	53+18	54+16
55− 1	56+10	57+14	58+17	59−14	60−11	61+ 2	62− 9	63+ 9
64− 6								
7−16	*4−17*	*11−14*	*10−11*	*24−28*	*12−13*	*7− 9*	*10−10*	*1−12*

обозначаетъ такую букву, которая занимаетъ въ азбукѣ мѣсто, равное алгебраической суммѣ X_1 и второго члена бинома. Очевидно, высшая сумма будетъ 28+12, т. е. X_1+12; низшая=64−6, т. е. X_1-6. Ясно, что X_1 не меньше шести, ибо послѣднее число оказалось возможнымъ изъ него вычесть; съ другой стороны, оно не больше 18, ибо къ нему прибавлено было двѣнадцать, что даетъ въ суммѣ 28, т. е. послѣднюю букву азбуки; значитъ X_1 больше 6; X_1 меньше 17; оно заключается между 7 и 16. Но если въ столбецъ попала хоть одна буква *а*, то $X_1=7$. (Ср. разсужденія въ главѣ VIII).

Такимъ же образомъ мы отыскиваемъ предѣлы для всѣхъ остальныхъ столбцовъ. Напр., въ IV столбцѣ высшій членъ $58+17=X_4+17$; высшій предѣлъ для X_4 оказывается 11 (28−17). Нисшій членъ $22-9=X_4-9$; нисшій предѣлъ=10; слѣдовательно, X_4 либо 10, либо 11. Для VIII столбца оба предѣла сливаются въ одинъ: $X_8=10$.

Предѣлы для всѣхъ буквъ ключа нанесены на табл. № 45 въ нижнемъ ряду.

Если бы мы по примѣру VIII главы, предположивъ во всѣхъ столбцахъ по буквѣ *а*, остановились для ключа на нисшихъ предѣлахъ, то получили бы совершенно неблагозвучное сочетаніе: „зглкшмжка“, которое свидѣтельствуетъ, что во многихъ столбцахъ нѣтъ совершенно буквы *а* *).

Приходится поэтому сдѣлать для каждой буквы ключа выборъ въ предѣлахъ максимума и минимума; для этого начнемъ съ тѣхъ, гдѣ предѣлы болѣе узкіе.

Напримѣръ, X_4 равно либо 10, либо 11; какое значеніе истинное? Замѣчаемъ въ столбцѣ двѣ разности „+3“, а такъ какъ буква *о* (=14) самая употребительная и обязательно попадетъ въ столбецъ, то предпочитаемъ 11, ибо 11+3 даетъ какъ разъ 14. Итакъ $X_4=11=$л. Далѣе, $X_5=24—28$. Нахожденіе въ V столбцѣ троекратнаго повторенія разности „−14“ заставляетъ думать, что $X_5-14=$ буквѣ *о*, т. е. $X_5=28=$я. Въ шестомъ столбцѣ, гдѣ $X_6=12—13$, мы находимъ разность „+1“, но нѣтъ разности „+2“, а потому выбираемъ $X_6=13=$н. Возьмемъ еще $X_7=7—9$. Такъ какъ X_8 безусловно равно 10=к, то X_7 можетъ быть только гласной, иначе мы имѣли бы совершенно невозможное по неблагозвучности стеченіе согласныхъ: „нж(з)к“. Слѣдовательно $X_7=9=$и. Найденная нами часть ключа составляетъ: ...ляник. Дальнѣйшій разборъ, еслибы мы даже и не отгадали остальныхъ буквъ, не представляетъ рѣшительно никакихъ затрудненій. Можно и опредѣлить остальныя буквы

*) Дѣйствительно, во всей криптограммѣ только два *а*. Чѣмъ меньше отрывокъ —а тутъ только 64 буквы, т. е. одна печатная строка—тѣмъ болѣе не только абсолютное уменьшеніе буквъ, но и возможное отступленіе отъ среднихъ нормъ, благодаря чему для однѣхъ перворазрядныхъ буквъ возможно скопленіе, для другихъ почти полное отсутствіе. Ничтожное количество здѣсь буквы *а* даетъ намъ возможность дополнить главу VIII, гдѣ пропорція *а* оказалась весьма благопріятной, и показать, какъ дѣйствовать и въ менѣе благопріятныхъ случаяхъ.

ключа, и поставить найденную часть въ текстъ, по методу, изложенному въ главѣ IX („сокращенный гамбеттовскій шифръ"). Ключъ: „земляника". Разобранный текстъ гласитъ: „Небо, до того времени голубое, вдругъ потускнѣло. Появились густыя сѣрыя облака". (Это начало текста изъ IX главы).

Чтобы покончить съ разборомъ, намъ приходится еще вернуться къ „вторичному періоду", или „числовому ключу". Мы раньше убѣдились, что, кромѣ „пятизначнаго ключа 23579, можно было бы предположить и десятизначный: 2.3.5.7.9., въ которомъ самыя существенныя цифры—стоящія на четныхъ мѣстахъ, слѣдовательно, падающія на всѣ вторые члены биномовъ,—остаются неизвѣстными. Такое обстоятельство неизбѣжно всякій разъ, когда для числового ключа взято число съ четнымъ количествомъ цифръ. Однако, и въ этомъ случаѣ возможно цѣликомъ опредѣлить ключъ, и мы для сокращенія изложенія покажемъ способъ открытія цифръ четнаго порядка на нашемъ же примѣрѣ, хотя въ немъ дѣйствительный ключъ, какъ мы видѣли, пятизначный.

Итакъ, допустимъ, что послѣднее обстоятельство оказалось несогласнымъ съ истиной, и что приходится перейти ко второму предположенію, что „числовой ключъ" десятизначный: 2.5.9.3.7. Въ немъ намъ неизвѣстны вторая, четвертая, шестая, восьмая и десятая цифры. Опредѣлимъ для примѣра четвертую. Для этого выпишемъ вторые члены всѣхъ биномовъ, на которые падетъ четвертая цифра ключа,—т. е. изъ 2-го, 7-го, 12-го, 17 и т. д. биномовъ. Получимъ рядъ: 7, 16, 11, 8, 16, 22, 17, 8, 22, 18, 24, 21, 16. Для сравненія приведемъ рядъ, который найдемъ для второй цифры ключа: 9, 4, 6, 7, 10, 8, 6, 13, 17, 5, 8, 13, 5. Въ первомъ минимумъ 7, во второмъ 4. Поэтому для четвертой цифры ключа надо допустить 7 или, пожалуй, 6; для второй же цифры 4, или, пожалуй, 3 *). Истинныя же цифры тутъ, какъ мы видимъ изъ нашего ключа 23579, для второго мѣста *3*, для четвертаго *7*.

Заключеніе. Потребовалось гораздо больше времени для описанія способа раскрытія „разностнаго гамбеттовскаго шифра съ двойнымъ періодомъ", чѣмъ для самаго раскрытія. Внѣшняя замысловатость оказывается дутой. Это одинъ изъ самыхъ ненадежныхъ шифровъ. Если же принять во вниманіе его тяжеловѣсность, то безъ всякихъ дальнѣйшихъ разговоровъ слѣдуетъ надъ нимъ поставить крестъ.

Глава XII.

СЛИТНЫЙ ПЕРІОДИЧЕСКІЙ ШИФРЪ

съ однороднымъ ключомъ.

Эта система представляетъ весьма существенное видоизмѣненіе гамбеттовскаго шифра, описаннаго въ VIII главѣ. Оно заключается въ томъ, что и первоначальный текстъ и ключъ при превращеніи въ числа пишутъ не раздѣльно (т. е. не отдѣляя другъ отъ друга числа, соотвѣтствующія отдѣльнымъ буквамъ), а *слитно*; сложеніе производится между двумя сплошными рядами цифръ, начиная, разумѣется, слѣва; въ случаѣ, если отъ сложенія цифры ключа и текста получается число, большее 9, то единицу десятковъ *переносятъ вправо* (а не влѣво, какъ при обыкновенномъ сложеніи); напр., знакомая уже намъ фраза „намъ нуженъ наборщикъ..." при ключѣ „шкурный вопросъ" изобразится такъ (по „тюремной азбукѣ"):

Раздѣльный текстъ:	13, 1, 12, 13, 19, 7, 6, 13, 13, 1, 2, 14, 16, 25, 9, 10...
Слитный текстъ:	131121319761313121416259 10...
Слитный ключъ:	+ 2410191613269314151614 1724...
Криптограмма:	37213057019725453657766644...

Особенности системы. При разгадкѣ всѣхъ предыдущихъ періодическихъ системъ (какъ и предшествовавшихъ шифровъ) всегда служило намъ опорнымъ ба-

*) Дѣло въ томъ, что въ первичномъ текстѣ обязательно долженъ попасть въ рядъ хоть одинъ биномъ типа $X+0$, или, по крайней мѣрѣ, $X\pm1$.

зисомъ раздѣленіе текста на *знаки*, соотвѣтствующіе разъединеннымъ буквамъ. Здѣсь мы этого рѣшительно не въ состояніи дѣлать: комбинаціи двузначныхъ и однозначныхъ чиселъ первичнаго текста и ключа при *поцифирномъ* сложеніи даютъ компактный рядъ, гдѣ совершенно исчезаютъ границы между буквами. Это обстоятельство до такой степени измѣняетъ дѣло, что даже при чтеніи съ ключомъ въ рукахъ, послѣ того какъ посредствомъ вычитанія получили слитный *первичный* текстъ, мы все же пребываемъ еще въ недоумѣніи, благодаря его слитности. Въ самомъ дѣлѣ. Положимъ, что продѣлавши поцифирное вычитаніе съ помощью ключа, мы получимъ рядъ: 316202823132915211328199133015291151675 30 *). Что это значитъ?

Въ дѣйствительности дѣло легче, чѣмъ кажется. Вспомнимъ, что высшее число въ полной азбукѣ—34 (я); поэтому разъ мы встрѣчаемъ сочетанія 35, 36, 37 и т. д., то они, значитъ, представляютъ соединеніе двухъ частей, принадлежащихъ *разнымъ* буквамъ, и разъединительная граница (цезура) должна пройти *внутри* такого сочетанія: 3 | 5; 3 | 6; 3 | 7... Далѣе, такъ какъ десятками могутъ здѣсь быть только 1, 2, 3, то всѣ остальныя цифры 4, 5, 6, 7, 9, 0 могутъ изображать собою только единицы, и потому цезура обязательно упадетъ справа отъ нихъ: 15 | 2..; 29 | 9 | ... Равнымъ образомъ, въ сочетаніяхъ 10, 20, 30 цезура не можетъ ихъ разрѣзывать, а должна упасть и слѣва и справа: ...1 | 20 | 11... На сто буквъ приходится до 81 цезуры, т къ что только 19 буквъ остаются невыдѣленными. Разставимъ цезуры въ вышезагаданномъ числовомъ ряду:

316 | 20 | 28 | 231329 | 15 | 211328 | 19 | 9 | 13 | 30 | 15 | 29 | 115 | 16 | 7 | 5 | 30.

Сомнительными остались только три небольшіе участка: 316, 231329 и 211328, что не можетъ служить препятствіемъ для прочтенія. Однако, во избѣжаніе всякихъ недоразумѣній, можно сдѣлать, напр., такое условное допущеніе. Такъ какъ подъ 10 (=і) и 30 (=ь) скрываются малоупотребительныя буквы, то можно выкинуть ихъ совсѣмъ изъ азбуки, а зато нуль ставить въ качествѣ цезуры *послѣ* 1 и 3. Три неразобранные еще участка были бы записаны тогда (а слѣдовательно и прочитаны) такъ: 3016, 23013029, 21013028 (фраза означаетъ: „вотъ хлынулъ сильный дождь").

Необходимость разставлять цезуры дѣлаетъ разбираемый шифръ не совсѣмъ удобнымъ для примѣненія. Писать текстъ, надписывать ключъ, производить сложенія, а при полученіи разставлять еще цезуры—отнимаетъ много времени; тутъ легко допустимы ошибки, описки. Затрудненія увеличиваются, если письмо не состоитъ изъ одного отрывка, а изъ нѣсколькихъ, или пишется не въ одинъ присѣстъ. Тутъ надо либо помнить, на какой цифрѣ ключа мы остановились при сложеніи, или же всякій разъ начинать ключъ съ начала. Если у насъ хранится записка съ нѣсколькими адресами, зашифрованными по этой системѣ, то если для каждаго адреса ключъ не брали съ начала, то для прочтенія одного адреса приходится всякій разъ начинать съ первой строчки. При такихъ неудобствахъ примѣненія требуется полная надежность для оправданія употребленія такой системы.

Задача. Вмѣсто сплошного текста предлагаемъ здѣсь шесть небольшихъ отрывковъ, представляющихъ начала шести адресовъ. При разбираемой системѣ *такой* случай представляетъ больше затрудненій, чѣмъ единичный отрывокъ (съ равнымъ количествомъ буквъ), такъ какъ тутъ нельзя изъ отрывковъ составить одинъ большой текстъ; этому мѣшаетъ періодичность системы. Цѣльную криптограмму мы разберемъ въ слѣдующей главѣ, гдѣ методы раскрытія тѣ же, что и въ настоящей.

1) 924284653605425806346836051428...
2) 903032564612579433354757035 0113...
3) 938619424703061845625825004 0092...
4) 982476433115514835747520185 2434...
5) 073526403633849795646837043 9788...
6) 953554423613039133354757035 0113...

Распознаваніе системы. Къ ней примѣнимо все то, что мы говорили о прерывистомъ квадратномъ шифрѣ съ фиктивными цифрами (см. гл. VI). Только съ нимъ ее и возможно смѣшать. Однако, отличіе выступаетъ сейчасъ же, какъ сдѣлаемъ подсчетъ цифръ. Дѣло въ томъ, что, какъ мы ниже покажемъ, здѣсь чаще всего встрѣчаются въ криптограммахъ цифры 2, 3, 4, 5, 6, причемъ максимумъ падаетъ на 3 и 4.

*) Здѣсь, какъ и во всѣхъ слѣдующихъ главахъ, мы пользуемся опять „полной" азбукой.

Въ прерывистомъ же квадратномъ отношенія знаковъ иныя. Суммируя цифры нашей „задачи“, находимъ:

1 2 3 4 5 6 7 8 9 0
14, *15*, *32*, *25*, *25*, *16*, 13, 13, 12, 20 разъ

Мы видимъ, что цифры 2—6 дѣйствительно встрѣчаются въ наибольшемъ количествѣ, общее число ихъ 113, тогда какъ на долю остальныхъ пяти цифръ приходится всего 72. Максимумъ приходится на 3—4. Слѣдовательно, діагнозъ несомнѣненъ.

Раскрытіе шифра. Оно основывается на специфическомъ распредѣленіи цифръ, на обязательномъ преобладаніи опредѣленныхъ цифръ. Первичный текстъ составляется изъ ряда чиселъ, не выходящихъ изъ предѣловъ 1—34. Такъ какъ десятками служатъ только 1, 2 и 3, то онѣ, естественно, будутъ чаще встрѣчаться, чѣмъ другія цифры. А такъ какъ буквы, соотвѣтствующія числамъ 10—19 (изъ „центральнаго“ отдѣла) гораздо употребительнѣе, чѣмъ буквы перваго и третьяго десятка, то цифра 1 будетъ самая частая. Изъ общаго числа 1658 цифръ, которыми въ среднемъ выражаются 1000 буквъ русской рѣчи, на долю 1 приходится 542, 2—238, 3—153, 4—64, 5—114, 6—182, 7—39, 8—101, 9—139, и 0—84 *). Такимъ образомъ, цѣлая треть всѣхъ цифръ состоитъ изъ единицъ. Очевидно, такія же отношенія, хотя и въ менѣе, можетъ быть, выраженной формѣ, будутъ и въ ключѣ. Напр., во взятомъ нами для образца ключѣ „шкурный вопросъ“ изъ 26 цифръ—девять единицъ.

Многочисленныя единицы и двойки ключа, падая на столь же частыя единицы и двойки, а также тройки первичнаго текста, дадутъ въ результатѣ преимущественное образованіе цифръ 2, 3, 4, 5, 6. Казалось бы, что максимумъ должна была бы дать цифра 2, какъ производная изъ двухъ единицъ (1+1); но дѣло въ томъ что при сложеніи часто получается результатъ больше 9 и приходится „переносить“ 1 къ слѣдующей суммѣ. Отъ этого часть двоекъ превратится въ тройки, и максимумъ перейдетъ на послѣднія.

Съ этими данными мы можемъ уже приступить къ рѣшенію „задачи“. На таблицѣ 46 всѣ 6 отрывковъ подписаны систематически одинъ подъ другимъ, образуя 31 столбецъ, пронумерованный римскими цифрами. Мы принимаемъ, что въ каждомъ изъ шести отрывковъ ключъ накладывался съ начала; еслибы то было иначе, еслибы второй отрывокъ составлялъ непосредственное продолженіе перваго, третій—второго и т. д., то тогда ихъ слѣдовало бы соединить вмѣстѣ въ одинъ текстъ и разобрать по методу, изложенному въ слѣд. главѣ.

Столбецъ I содержитъ въ себѣ шесть цифръ: 9, 9, 9, 9, 0, 9, получившихся отъ сложенія съ одной и той же цифрой ключа—X_1. Переноса единицы слѣва тутъ еще не можетъ быть, ибо это *первый* столбецъ, но, конечно, возможенъ переносъ единицы де-

*) При этомъ принималась во вниманіе и буква ъ. Безъ нея 2 встрѣчается только 198 разъ, 8—53. Общее число цифръ 1560, а буквъ—952. По этимъ даннымъ мы и произвели расчетъ „цезуръ“.

Таблица № 46.

	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}	X_{22}	X_{23}...
	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV	XVI	XVII	XVIII	XIX	XX	XXI	XXII	XXIII
1)	9	2	4	2	8	4	6	5	3	6	0	5	4	2	5	8	0	6	3	4	6	8	3
2)	9	0	3	0	3	2	5	6	4	6	1	2	5	7	9	4	3	3	3	5	4	7	5
3)	9	3	8	6	1	9	4	2	4	7	0	3	0	6	1	8	4	5	6	2	5	8	2
4)	9	8	2	4	7	6	4	3	3	1	1	5	5	1	4	8	3	5	7	4	7	5	2
5)	0	7	3	5	2	6	4	0	3	6	3	3	8	4	9	7	9	5	6	4	6	8	3
6)	9	5	3	5	5	4	4	2	3	6	1	3	0	3	9	1	3	3	3	5	4	7	5
	8	?	1	3/4	1/6	3	3	1/4	1/2	5	9	1	3	1	8	6	1	4	1/5	3	3	6	1/2

	XXIV	XXV	XXVI	XXVII	XXVIII	XXIX	XXX	XXXI
1)	5/6	9	1	2/4	8	4	2	8...
2)	7	0	3	5	0	1	1	3...
3)	5	0	0	4	0	0	9	2..
4)	1	0	8	5	2	4	3	4..
5)	6	0	4	3	9	7	8	8...
6)	7	0	3	5	0	1	1	3...
	8	8	6	1	8	8	6	1

сятковъ вправо, ко второму столбцу. Мы знаемъ уже, что цѣлая треть первичнаго текста состоитъ изъ цифры 1, слѣдовательно изъ шести цифръ, по крайней мѣрѣ, *двѣ* будутъ таковыя и, сложенныя съ X_1, дадутъ въ результатѣ одинаковыя цифры. Въ I столбцѣ ихъ имѣется цѣлыхъ пять (9); ясно, что это и есть сумма X_1 съ единицей текста; $X_1=8$. А цифра 0 =10 и представляетъ сумму X_1 съ двойкой, которая тоже имѣется въ текстѣ въ большомъ количествѣ. Очевидно, въ пятомъ ряду единица десятковъ перенесена во второй столбецъ, и истинная сумма тамъ будетъ не 7, а 6.

Столбецъ II содержитъ: 2, 0, 3, 8, *7*, 5; истинный составъ: 2, 0, 3, 8, *6*, 5. Здѣсь не оказывается двухъ одинаковыхъ цифръ; въ такомъ случаѣ имѣетъ значеніе наличность двухъ или болѣе послѣдовательныхъ чиселъ, напр., 3, 2; 6, 5, 4 и т. п. Дѣло въ томъ, что, кромѣ 1, въ текстѣ весьма часто встрѣчаются, какъ мы видѣли, 2 и 3, и сумма этихъ послѣдовательныхъ чиселъ съ одной и той же цифрой ключа дастъ тоже послѣдовательный рядъ цифръ. Впрочемъ, и съ этимъ мы во II столбцѣ далеко не уѣдемъ, такъ какъ онъ не заключаетъ въ себѣ ничего опредѣленнаго: X_2 остается неизвѣстной. Важно все таки замѣтить, что она выражается, приблизительно, въ сферѣ 6—5—4 (это имѣетъ значеніе для исправленія III столбца отъ „переноса").

Столбецъ III: 4. 3, 8, 2, 3, 3, исправленный: *3*, *2*, 7, *2*, *3*, *3*. Курсивомъ отмѣчены тѣ цифры, которыя служатъ для опредѣленія X_3; $X_3=1$.

Столбецъ IV: 2, 0, *6*, *4*, *5*, *5*; $X_4=4$ (а можетъ быть 3).

Столбецъ V: 8, 3, 1, 7, 2, 5. Исправленный: 7. 2, 1, 7, 2, 5; $X_5=6$ или 1.

Столбецъ VI: *4*, 2, 9, 6, 6, *4*; $X_6=3$.

Столбецъ VII: 6, 5, 4, 4, 4, 4. Исправленный: 6, 4, 4, 4, 4, 4; $X_7=3$.

Столбецъ VIII: 5, 6, 2, 3, 0, 2; $X_8=1$ (но возможно и 4).

Столбецъ IX: 3, 4, 4, 3, 3, 3. Исправленный: 1) 3, 4, 4. 3, 2, 3; 2) 3, 4, 3, 2, 2, 2; $X_9=1$ или 2.

Столбецъ X: 6, 6, 7, 1, 6. 6; $X_{10}=5$.

Столбецъ XI: 0, 1, 0, 1, 3, 1. Исправленный: 0, 1, 0, 0, 3, 1; $X_{11}=9$.

Столбецъ XII: 5, 2, 3, 5, 3, 3. Исправленный: 4, 1, 2, 4, 2, 2; $X_{12}=1$.

Столбецъ XIII: 4, 5, 0, 5, 8, 0; $X_{13}=3$.

Столбецъ XIV: 2, 7, 6, 1, 4, 3. Исправленный: 2, 7, 5, 1, 4, 2; $X_{14}=1$.

Столбецъ XV: 5, 9, 1, 4, 9, 9; $X_{15}=8$.

Столбецъ XVI: 8, 4. 8, 8, 7, 1. Исправленный: 7. 4, 7, 7, 7, 1; $X_{16}=$*6*.

Столбецъ XVII: 0, 3, 4, 3, 9, 3. Исправленный: 0, 2, 4, 3, 9, 2; $X_{17}=1$.

Столбецъ XVIII: 6, 3, 5, 5. 5, 3. Исправленный: 5, 3, 5, 5, 5, 3; $X_{18}=4$.

Столбецъ XIX: 3, 3, 6, 7, 6, 3. Исправленный: 3, 2, 6, 7, 6, 2; $X_{19}=1$ или 5.

Столбецъ XX: 4, 5, 2, 4, 4. 5; $X_{20}=3$.

Столбецъ XXI: 6, 4, 5, 7, 6, 4. Исправленный: 6, 4, 4, 7, 6, 4; $X_{21}=3$.

Столбецъ XXII: 8, 7. 8, 5, 8, 7; $X_{22}=6$.

Столбецъ XXIII: 3, 5, 2, 2, 3, 5. Исправленный: 3, 5, 2, 1, 3, 5; $X_{23}=1$ (2, 4).

и т. д.

Разультаты нанесены на табл. № 46 въ нижнемъ ряду. Присматриваясь къ этому ряду, мы замѣчаемъ явную періодичность, повтореніе одинаковыхъ группъ, напр.: 814; 8614; 861. Точно также: 33 и 33; 91 и 91. Одинаковыя сочетанія *всѣ* отстоятъ другъ отъ друга на 14 цифръ. Слѣдовательно, періодъ состоитъ именно изъ такого количества цифръ. Раздѣлимъ нижній рядъ на грани изъ 14 цифръ и подпишемъ одну подъ другой:

8; —; 1; 4; $^1/_6$; 3; 3; $^1/_4$; 1; 5; 9, 1; 3; 1
8; 6; 1; 4; $^1/_5$; 3; 3; 6; $^1/_2$; $^5/_6$; 9, 1; $^2/_4$; 8
8; 6; 1...

Ключъ: 8; 6; 1; 4; 1; 3; 3; ?; 1; 5; 9; 1; ?; $^1/_8$

Сопоставленіе двухъ-трехъ рядовъ разрѣшило вопросъ относительно нѣсколькихъ сомнительныхъ цифръ. Остались невыясненными еще 3 цифры ключа.

Разставимъ цезуры:

8—6—14—133?15—9—1?$^1/_8$.
з е м л н и а/з

Ясно, что ключъ „земляника". Сомнительныя цифры: 4 (выборъ былъ изъ 1, 4, 6), 2 (выборъ: 2, 3, 4) и 1 (выборъ: 1, 8). Числовое выраженіе ключа: 86141334159121.

Остается лишь вычесть ключъ изъ всѣхъ отрывковъ „задачи", разставить цезуры подставить буквы. Прочтемъ:

1) Орел Калужская улица..
2) Москва Тверская улица...
3) Петербург Владимирска...
4) Кіев Сольскому до вост...
5) Тула Самоварная фабрика...
6) Самара Казанская улица...

Заключеніе. Такимъ образомъ, практическія неудобства этой системы, затруднительность ея примѣненія совершенно не окупаются съ точки зрѣнія надежности. Поэтому шифръ этотъ никоимъ образомъ не можетъ быть рекомендованъ.

Глава XIII.

СЛИТНЫЙ ПЕРІОДИЧЕСКІЙ ШИФРЪ

съ разнороднымъ ключомъ.

Тѣхъ же щей...

Предыдущая система представляетъ тотъ недостатокъ, что и первичный текстъ и ключъ, благодаря способу своего составленія, обладаютъ заранѣе извѣстнымъ распредѣленіемъ цифръ (преобладаніе 1, 2 и т. д.). Здѣсь же дѣлается попытка уничтожить этотъ недостатокъ, по крайней мѣрѣ, въ числовомъ ключѣ, который получается инымъ способомъ, чѣмъ раньше.

Пусть ключомъ служитъ: „пкурный вопрос". Составимъ по немъ числовой распредѣлитель такъ, какъ это дѣлается въ сложныхъ квадратныхъ шифрахъ (см. главу V) съ той лишь разницей, что *одинаковыя* буквы обозначимъ *одинаковыми* цифрами (а не послѣдовательными); затѣмъ, такъ какъ тутъ число буквъ больше десяти, то вмѣсто 11 напишемъ 1, вмѣсто 12 — 2 и т. д. (можно условиться писать и сумму цифръ, т. е, вмѣсто 11 — 2 (1 + 1), вмѣсто 12 — 3 (1 + 2) и т. д.). Такимъ образомъ получимъ такое число:

п к у р н ы й в о п р о с
0 3 9 7 4 1 2 1 5 6 7 5 8

Составленное по такому способу число не обладаетъ тѣми специфическими особенностями, какія имѣетъ ключъ въ предыдущемъ шифрѣ: тутъ нѣтъ преобладанія 1 и 3.

Особенности системы. Усовершенствованіе это дѣлаетъ невозможнымъ распознаваніе системы по прежнему способу, ибо въ криптограммѣ ужъ не будетъ обязательнаго преобладанія цифръ 2, 3, 4, 5, 6 съ максимумомъ на 3 и 4 (ср. пред. главу). Точно также здѣсь невозможно или трудно по извѣстнымъ частямъ ключа возстановить неизвѣстныя, ибо распредѣленіе цифръ въ немъ совершенно искусственное. Но все-таки тутъ не уничтоженъ основной недостатокъ — специфичность первичнаго текста.

Задача. 87886202728129919131585815089146007502290984715827353288440534695509739565463889134957821069923233644135018551558 49.

Распознаваніе системы. Сдѣлавъ подсчетъ цифръ, находимъ, что общее число ихъ 115 распредѣляется такъ:

1, 2, 3, 4, 5, 6, 7, 8, 9, 0
12, 11, 11, 10, 17, 7, 7, 16, 14, 10 (разъ).

Отличіе отъ предыдущей системы дѣлается сразу, ибо тутъ нѣтъ характернаго преобладанія цифръ 2 — 6. Что касается прерывистаго квадратнаго (съ фиктивными цифрами), съ которымъ только и возможно ее смѣшать, то отличительные признаки послѣдняго изложены уже выше (см. гл. VI).

Раскрытіе шифра. Если на первичный текстъ, отличающійся, какъ намъ уже извѣстно, специфическимъ составомъ, наложить ключъ, содержащій всѣ цифры и притомъ поровну, состоящій, слѣдовательно, изъ 10, 20, 30 и т. д. цифръ, то нетрудно понять, что въ криптограммѣ цифры должны встрѣчаться приблизительно равномѣрно, а въ особенности равномѣрными должны оказаться суммы двухъ рядомъ стоящихъ цифръ (напр., единицъ и двоекъ, троекъ и четверокъ и т. д.). Хотя цѣлая треть первичнаго текста состоитъ изъ единицъ, но такъ какъ онѣ распредѣляются приблизительно поровну между десятью различными цифрами ключа, то онѣ дадутъ приблизительно поровну 1, 2, 3, и т. д. Тоже будетъ съ двойками первичнаго текста, съ тройками и т. д. Если же въ ключѣ нѣкоторыя цифры повторяются, напримѣръ, имѣются двѣ четверки, то благодаря преобладанію въ текстѣ единицъ, получится избыточное количество цифры 5 (а также 6 — благодаря „переносу"). Въ нашемъ текстѣ имѣется много 8 и 9, что заставляетъ предполагать повторность въ ключѣ цифры *7*.

Прежде всего намъ необходимо узнать періодъ, т. е. сколько цифръ въ ключѣ. Мы уже знаемъ, что во всѣхъ разобранныхъ нами періодическихъ системахъ замѣчается извѣстная степень періодичности одинаковыхъ знаковъ, повторяемость ихъ въ вертикальныхъ столбцахъ табл. 36 и 40. То же самое должно быть и здѣсь; въ особенности это относится къ такимъ знакамъ, какъ 8 и 9 (въ нашей „задачѣ"), потому что преобладаніе ихъ прямо обусловливается нахожденіемъ въ ключѣ лишней *7*, а слѣдовательно въ ихъ распредѣленіи непремѣнно долженъ отразиться періодъ. Чтобы получить болѣе рельефный результатъ, мы свалимъ въ одну кучу и 8, и 9 и изучимъ распредѣленіе всѣхъ 30 цифръ, ибо, благодаря „переносу", трудно отдѣлить другъ отъ друга смежныя цифры. Эти 30 цифръ занимаютъ въ „задачѣ" слѣдующія мѣста: 1, 3, 4, 11, 14, 15, 17, 22, 24, 28, 29, 40, 42, 43, 48, 55, 56, 64, 68, 71, 78, 79, 80, 84, 87, 92, 93, 107, 113 и 115-ое. Находимъ промежутки между ними („разности") такъ, какъ мы это дѣлали въ гл. IX и XI, и наносимъ ихъ на таблицу 47, аналогичную таблицамъ 39 и 44. Опредѣлять разности для *всѣхъ* знаковъ, т. е. для 1, 2 и т. д., нѣтъ надобности.

Таблица № 47.

	0	1	2	3	4	5	6	7	8	9
0	—	8	6	7	3	6	6	7	7	5
1	5	7	8	12	11	6	6	1	6	4
2	6	6	2	8	7	7	9	6	8	7
3	1	6	5	3	3	3	7	8	5	8
4	5	6	5	2	7	5	1	6	—	7
5	5	6	5	4	4	3	4	4	3	3
6	4	2	3	4	6	7	2	5	3	3
7	5	2	2	4	1	4	4	3	4	3
8	1	2	1	3	2	2	2	1	1	3
9	2	3	2	2	—	—	2	—	2	1
10	1	1	1	1	2	—	1	—	—	1
11	1	1	2	—	1	—	—	—	—	—

Выпишемъ и здѣсь самыя частыя разности:

12 разъ: *13*.
11 „ 14.
9 „ *26*.
8 „ 1, 12, 28, 37, *39*.
7 „ 7, 8, 11, 24, 25, 29, 36, 44, 49, *65*.

Ясно, что періодъ заключается въ рядѣ 13, 26, 39, 65, гдѣ всѣ числа кратны 13. Слѣдовательно, ключъ содержитъ тринадцать цифръ. Провѣряя на частотѣ остальныхъ разностей, кратныхъ 13, находимъ, что:

Разности 13, 26, 39, 52, 65, 78, 91, 104
встрѣчаются 12, 9, 8, 5, 7, 4, 3, 2 раза.

Дѣлимъ теперь, конечно, криптограмму на грани по 13 цифръ и подписываемъ ихъ одну подъ другой, аналогично таблицамъ 40 и 45 (см. табл. № 48).

Въ дальнѣйшемъ поступаемъ совершено такимъ же образомъ, какъ въ предыдущей главѣ. Напр., I-й столбецъ, содержащій 0, 0, 9, 9, 9, 8, 8, 5, 3, несомнѣнно имѣетъ соотвѣтствующую цифру ключа -7. Второй столбецъ (послѣ поправки): 7, 9, 7, 0, 1, 9, 9, 9, 9,—въ ключѣ 8; и т. д., и т. д. Цифры ключа въ томъ видѣ, какъ онѣ выступаютъ при обзорѣ столбцовъ, нанесены на таблицѣ № 48 въ нижнемъ ряду. Двѣ сомнительныя цифры опредѣляются вполнѣ точно изъ первой же подстановки въ текстѣ.

Ключъ: 7867219351604—отъ слова „основательный". Разобранный текстъ гласитъ: „Самара. Казанская улица, домъ графа Шувалова, квартира третья, Андрею Никодимичу Эртелю" (тотъ же текстъ, что въ главѣ VIII).

Таблица № 48.

	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII
А	8	7	8	8	6	2	0	2	7	2	8	1	2
Б	9	9	1	9	1	3	1	5	8	5	8	1	5
В	0	8	9	1	4	6	0	0	7	5	0	2	2
Г	9	0	9	8	4	7	1	5	8	2	7	3	5
Д	3	2	8	8	4	4	0	5	3	4	6	9	5
Е	5	0	9	7	3	9	5	6	5	4	6	3	8
Ж	8	9	1	3	4	9	5	7	8	2	1	0	6
З	9	9	2	3	2	3	3	6	4	4	1	3	5
И	0	1	8	5	5	1	5	5	8	4	9		
	7	8	6	7/6	2	1	9	3	5	1	6/5	0	4

Заключеніе. Мы видимъ, слѣдовательно, что „усовершенствованіе“ здѣсь совершенно не достигаетъ цѣли, и вмѣстѣ съ нимъ шифръ такъ же непригоденъ, какъ безъ него.

Глава XIV.

ВТОРИЧНЫЙ СЛИТНЫЙ ШИФРЪ.

(Комбинація съ квадратнымъ).

Красивъ мой домъ, по плану онъ построенъ,
Но, ахъ, подъ нимъ нетвердо основанье!

Шиллеръ, „Вильгельмъ Телль“.

Онъ состоитъ въ томъ, что числовой ключъ накладывается на предварительно *зашифрованный по другой системѣ* текстъ, иными словами, это—комбинація періодическаго шифра съ какимъ-нибудь инымъ, напр., квадратнымъ. Положимъ, что фраза: „намъ нуженъ наборщикъ...“ зашифрована сперва простымъ квадратнымъ шифромъ по ключу „начальникъ“, а потомъ криптограмма измѣнена посредствомъ періодическаго наложенія числа 0397412156758, полученнаго съ помощью фразы: „пкурный вопросъ“ (см. гл. XIII).

Первичная криптограмма . . 532193119027467153210972803381 91...
Періодъ . . . . . 0397412156758039741215675803 9741...

Вторичная криптограмма . . 561935324792370138331440494679 32...

Такова разбираемая система. Разумѣется, вмѣсто простого квадратнаго, можно брать для первичной криптограммы и сложный, и прерывистый, и множественный квадратный, вообще всякій шифръ, выражающійся *числомъ*, а не буквами (стало быть и книжный, и стихотворный—см. гл. XV и XVI).

Особенности системы. Здѣсь исчезаетъ и второй, самый опасный недостатокъ слитнаго періодическаго шифра—специфичность состава первичнаго текста. Послѣдній является тутъ совершенно неизвѣстнымъ ни со стороны системы, ни со стороны распредѣленія цифръ; во всѣхъ отношеніяхъ—полнѣйшій иксъ. Это обстоятельство дѣлаетъ разгадку невозможной еще и потому, что мы не можемъ уже сомнительныя

цифры періода провѣрять посредствомъ подстановки въ текстѣ, какъ мы дѣлали въ предыдущихъ главахъ. Первичный текстъ представляетъ нѣчто глухое, ничего не говорящее, долженствующее еще быть, въ свою очередь, разобраннымъ. Итакъ, нѣтъ ничего, на что можно было бы опереться при анализѣ, и потому шифръ является однимъ изъ самыхъ недоступныхъ.

Задача. 691139278635289572044982235954979457594297306550186295887424153352480985036482267698114439632172115031236663175178678025696345743553636800179681418959345617839690170510399007856498155659118675561346218811569398491057836996827825018039600488342666670764215993786087474037418608837841337126650739508959346165836666954309397092656777159949410091731454812994328156741274011035133993420229636584851937468853092262057229105352900161276238162172145703083 9.

Распознаваніе системы. Неизмѣнно четное количество цифръ, какъ въ совокупности, такъ и въ каждомъ отдѣльномъ отрывкѣ, и вообще внѣшній видъ заставляетъ предполагать квадратный шифръ. Сдѣлавъ подсчетъ всѣхъ 224 знаковъ (табл. № 49), придемъ къ заключенію, что имѣемъ дѣло съ сложнымъ квадратнымъ шифромъ, и только послѣ того, какъ всѣ попытки разобрать его потерпятъ фіаско, тогда только можно заподозрить комбинацію его съ періодическимъ.

Таблица № 49.

	1	2	3	4	5	6	7	8	9	0
1	5	1	2	2	2	2	4	1	1	4
2	4	1	2	1	2	2	2	1	3	—
3	1	1	2	3	3	—	2	1	8	1
4	4	2	1	1	1	2	1	1	3	1
5	1	2	3	3	—	5	3	—	5	3
6	2	3	5	3	5	4	3	1	3	2
7	1	4	1	4	1	1	1	5	—	1
8	3	3	4	1	3	3	1	3	2	2
9	1	1	3	3	3	4	2	3	—	3
0	3	1	2	2	2	—	4	2	2	2

Раскрытіе шифра. Прежде всего надо, разумѣется, узнать періодъ. Распознаваніе его здѣсь основывается на изученіи повторныхъ знаковъ. Мы знаемъ уже, что въ квадратныхъ шифрахъ знаки, выражающіе болѣе частыя буквы, неизмѣнно повторяются. При наложеніи періода, на нихъ будутъ *вообще* падать различныя части его, и потому они не только измѣнятся до неузнаваемости, но и другъ на друга перестанутъ походить. Напримѣръ, во взятой нами выше для образца фразѣ оказались повторенными по два раза 53 и 21. Но такъ какъ на нихъ упали нетождественныя части ключа, то вмѣсто 53, 53 получилось 56 и 38, а вмѣсто 21, 21 — 19 и 23. Но если бы на нихъ упала одна и та же часть ключа, то и во вторичной криптограммѣ оказались бы *одинаковыя* двузначныя числа (а иногда *почти* одинаковыя, благодаря измѣненіямъ, вносимымъ „переносомъ"). При достаточно большомъ отношеніи величины текста къ размѣрамъ періода такіе случаи совпаденія неизбѣжны, почему изученіе взаимнаго положенія повторяющихся знаковъ можетъ открыть длину *періода*. Послѣдній различенъ для ключей съ четнымъ и нечетнымъ количествомъ цифръ. Если въ ключѣ четное число ихъ, напр. 18, то каждая изъ его 9 паръ цифръ всегда будетъ падать на парный знакъ первичнаго текста, періодъ будетъ здѣсь — 9, и въ разстояніяхъ между повторяющимися числами криптограммы будетъ по преимуществу отражаться число 9. Если же въ ключѣ нечетное число цифръ, напр. 17, то лишь въ половинѣ случаевъ пары ключа будутъ падать на парные знаки текста, въ другой половинѣ случаевъ онѣ будутъ ихъ разрѣзывать, поэтому лишь о *двойномъ* ключѣ (содержащемъ, слѣдовательно, 34 цифры или 17 паръ) можно сказать, что его пары будутъ всегда совпадать со знаками текста. Періодъ здѣсь 17.

Итакъ, пронумеруемъ всѣ знаки (т. е. пары) „задачи", выберемъ всѣ повторяющіеся и опредѣлимъ ихъ разности по извѣстному уже намъ методу.

Знакъ „59".

Мѣста въ текстѣ: 14, 19, 93, 128, 150

Разности. 5, 79, 114, 136
74, 109, 131
35, 57
22

Знакъ „27“.

Мѣста въ текстѣ: 4. 214

Разность 210

Результатъ суммируемъ на таблицѣ № 50, аналогичной табл. № 47.

Выписываемъ болѣе частыя разности:

6 разъ: *5*, 8.
5 „ 13, *15*, *75*.
4 „ 27, *30*, 59, *100*, 103.
3 „ 23, 28, 31, 33, 39, *40*, 41, *45*, *60*, 63, 101, 109, *130*, 171.

Находимъ рядъ: 5, 15, 75, 30, 100, 40, 45, 60, 130, изъ котораго вполнѣ очевидно, что періодъ составляетъ число 5. Провѣрка по остальнымъ членамъ этого ряда (10, 20, 25 и т. д.) вполнѣ подтвердитъ нашъ результатъ. Теперь возможны два случая. Если въ неизвѣстномъ намъ ключѣ число цифръ четное, то оно равно 10 (5×2), если же нечетное, то 5. Благоразумнѣе взять для первой пробы 10, ибо пять слишкомъ малое число.

Таблица № 50.

	0	1	2	3	4	5	6	7	8	9
0	—	1	1	—	2	6	2	—	6	1
1	2	2	2	5	1	5	2	1	1	1
2	1	2	2	3	—	1	2	4	3	1
3	4	3	2	3	1	2	1	1	1	3
4	3	3	2	1	1	3	—	2	1	2
5	—	2	1	2	1	—	2	2	—	4
6	3	1	2	3	1	—	1	—	1	1
7	1	1	2	3	1	5	—	2	1	1
8	2	—	1	2	—	2	—	1	2	1
9	2	1	2	—	—	1	2	1	1	—
10	4	3	2	4	—	—	1	2	2	3
11	1	—	—	—	2	1	—	1	1	1
12	—	1	2	—	2	1	1	—	—	—
13	3	2	1	—	—	1	1	—	—	2
14	1	—	—	2	1	—	1	1	—	1
15	—	—	1	—	1	—	—	2	1	1
16	2	—	—	—	—	—	—	1	—	—
17	1	3	1	—	—	—	—	2	1	1
18	1	—	—	—	—	1	—	—	—	1
19	—	—	—	—	—	—	—	1	1	—
20	—	—	—	—	—	—	—	—	—	—
21	2	—	—	—	—	—	—	—	—	—

Раздѣлимъ нашу задачу на грани по 10 цифръ въ каждой и подпишемъ одну подъ другой. Мы получимъ тогда 45 рядовъ по 10 цифръ въ каждомъ (всего 448 цифръ) или 10 вертикальныхъ столбцовъ по 45 цифръ. Подсчитаемъ въ каждомъ изъ 10 столбцовъ количество единицъ, двоекъ, троекъ и т. д. и нанесемъ результаты на табл. № 51.

Дальнѣйшій анализъ будетъ довольно сложенъ и потому понадобится усиленное вниманіе со стороны читателя.

Вообразимъ, что въ первичной криптограммѣ *самой частой цифрой* является Z (обыкновенно она совпадаетъ со столбцомъ ключа въ квадратныхъ шифрахъ). Очевидно, что по раздѣленіи первичнаго текста на грани по 10 цифръ и послѣ того, какъ онъ будетъ представленъ въ видѣ десяти вертикальныхъ столбцовъ, эта самая частая цифра Z будетъ преобладать и въ каждомъ столбцѣ. Сложенная съ соотвѣтствующей цифрой періода она дастъ максимальное количество (M) другой цифры, напр., Y; или же, въ случаѣ многихъ „переносовъ“, окажутся большими двѣ послѣдовательныя цифры Y и Y+1. Очевидно, Y получится тогда, когда предыдущая цифра ключа (X) маленькая, напр. 0, 1, 2, а Y и Y+1 въ томъ случаѣ, когда она большая, напр., 7, 8, 9.

Таблица № 51.

	I X_1	II X_2	III X_3	IV X_4	V X_5	VI X_6	VII X_7	VIII X_8	IX X_9	X X_{10}
0	2	6	5	2	3	3	4	5	6	3
1	2	5	8	7	5	5	3	5	6	3
2	1	3	7	4	3	4	4	4	3	4
3	7	3	5	9	4	4	1	9	5	—
4	4	7	—	2	5	3	6	6	2	6
5	4	6	3	2	7	7	5	2	6	4
6	7	4	3	7	11	3	6	3	4	6
7	6	4	2	3	4	6	4	5	3	5
8	3	2	5	3	2	5	9	1	6	7
9	9	5	7	6	1	5	3	5	3	6
	3	8	5	6	0	9	1	7	4	2

Для примѣра возьмемъ десятый столбецъ (№ X); въ немъ два максимума (M): 7 и 6 соотвѣтствующіе двумъ послѣдовательнымъ цифрамъ (Y и Y + 1) — 8 и 9 Цифра ключа здѣсь обозначена X_{10}. Выберемъ самый рельефный столбецъ перваго типа (т. е. съ однимъ максимумомъ); это будетъ № I, такъ какъ въ немъ M - 9 лежитъ между двумя маленькими числами 3 и 2. Мы изъ этого заключаемъ, что въ предшествующемъ столбцѣ (№ X) цифра ключа X_{10} маленькая, въ предѣлахъ 0—2. А такъ какъ въ № X максимумъ падаетъ на цифру 8 (иными словами, Y=8), которая полу-

чилась, очевидно, отъ сложенія X_{10} съ Z, то составляемъ такое уравненіе: $Z=8-X_{10}=8-(0-2)$; $Z=6-8$; Z заключается между 6 и 8.

Но если мы разыщемъ другой вполнѣ рельефный и выраженный столбецъ того же типа, именно № IV, гдѣ M (7) лежитъ между двумя тройками, то получимъ для Z другіе предѣлы. Въ предыдущемъ—V столбцѣ Y=6, X_5 тоже заключается между 0—2; $Z=6-X_5=6-(0-2)=4-6$; Z заключается между 4 и 6.

Аналогичныя границы для Z мы найдемъ, если возьмемъ пару самыхъ выраженныхъ столбцовъ второго типа, напр. № IX, гдѣ имѣется два M—6, 6 (Y, Y+1). Заключаемъ, что въ предыдущемъ VIII столбцѣ X_8 — большая цифра въ предѣлахъ 7—9; а такъ какъ тамъ Y=3 (13), то $Z=13-X_8=13-(7-9)$; Z=4—6 (между 4 и 6).

Другой же столбецъ второго типа—№ III, гдѣ M=8+7; такъ какъ въ предыдущемъ № II Y=4 (14), то $Z=14-X_2=14-(7-9)$; Z=5—7 (между 5 и 7).

Итакъ, для Z мы нашли такіе предѣлы: оно заключается между 4 и 6, между 5 и 7, между 6 и 8. Ясно, что Z=6; это значитъ, что въ первичной криптограммѣ самой частой цифрой является 6.

Теперь предстоитъ задача отыскать цифры ключа, т. е. значенія X_1, X_2, X_3 и т. д. Начнемъ съ болѣе выраженныхъ столбцовъ.

Въ № IX: =9 (10); это число получилось, какъ результатъ сложенія цифры ключа X_9 съ Z. Слѣдовательно. $X_9=10-Z=10-6=4$.

Въ № X: Y=8; $X_{10}=8-Z=8-6=2$.

Въ № I: Y=9; $X_1=9-6=3$.

Въ № II: Y=4 (14); $X_2=14-6=8$.

Въ № III: Y=1 (11); $X_3=11-6=5$.

Въ № IV: Y, повидимому, 3, такъ какъ коэффиціентъ тутъ максимальный—9, но такъ какъ въ предшествующемъ столбцѣ X_3—большая цифра (5), дающая много „переносовъ", то разумнѣе признать 3 за Y+1, а за Y принять 2, хотя тамъ коэффиціентъ всего 4. Итакъ, Y=2 (12); $X_4=12-6=6$.

Въ № V: =6; $X_5=6-6=0$ *).

Въ № VI: =5 (15); $X_6=15-6=9$.

Въ № VII: за Y принимаемъ 7, а не 8, по той же причинѣ, что въ столбцѣ № IV; $X_7=7-6=1$.

Въ № VIII: Y=3 (13); $X_8=13-6=7$.

Весь періодъ составляетъ 3856091742.

Если теперь вычитать послѣдовательно цифры періода изъ „задачи", то получимъ новую криптограмму (первичную), состоящую, конечно, изъ 448 цифръ. Сдѣлавши подсчетную таблицу знаковъ (таблица № 52), найдемъ, что въ основѣ былъ положенъ сложный квадратный шифръ, въ которомъ, очевидно, ключъ расположенъ въ столбцѣ 6-омъ. Раскрывать его мы здѣсь не станемъ, такъ какъ этому шифру уже посвящена глава V.

Таблица № 52.

	1	2	3	4	5	6	7	8	9	0
1	3	5	3	2	—	—	5	—	—	1
2	2	—	4	—	3	3	1	—	3	4
3	2	6	2	4	2	7	1	3	3	—
4	—	3	1	4	1	6	3	6	—	7
5	2	3	1	—	4	4	7	1	1	1
6	3	8	4	9	3	6	1	3	5	—
7	1	3	2	—	—	3	—	2	1	—
8	1	2	1	1	—	9	—	—	—	1
9	.	2	1	—	—	3	—	1	4	—
0	—	—	—	3	2	4	2	3	2	4

Разобранный текстъ гласитъ: „Подъ безпредѣльнымъ синимъ шатромъ тихо сіяли вершины горъ, отчетливо выступали разбросанныя селенія, тонкой восковой свѣчкой свѣтилась между полями колокольня, и вся даль, ясная, чудная даль смотрѣла кротко и задумчиво... Вверху радостно и на всѣ лады звенѣли невидимые пѣвцы".

Ключемъ послужило здѣсь „ЯрославльЩ", написанное снизу вверхъ. Распредѣлителемъ слово „Петербургъ"—по вторичному способу. Періодъ составленъ по слову „исключеніе".

Приводимъ здѣсь для сравненія количества цифръ въ первичной и вторичной криптограммахъ:

---

*) Мы имѣли бы право и здѣсь разсуждать, какъ въ № V, и принять за Y—5, а не 6; тогда $X_5=15-6=9$. Но мы уже выше видѣли, при разборѣ № VI, что въ пятомъ столбцѣ X_5 малая цифра, а это возможно лишь когда Y=6.

	1,	2,	3,	4,	5,	6,	7,	8,	9,	0.	Итого
Первичная:	33,	52,	49,	54,	39,	87,	32,	34.	30,	38	= 448.
Вторичная:	49,	37,	47,	40,	47,	54,	42,	43,	50,	39	= 448.

Заключеніе. Вторичный періодическій шифръ безусловно самый надежный изъ всѣхъ разобранныхъ системъ. Во-первыхъ, если взять достаточно длинный періодъ, то даж^ф определеніе его длины можетъ стать невозможнымъ. Во-вторыхъ, все раскрытіе основано на томъ, что въ первичномъ текстѣ одна какая-нибудь цифра значительно преобладаетъ надъ остальными. Но этого можетъ и не случиться, а при равномѣрномъ распредѣленіи цифръ разгадка становится невозможной. Въ-третьихъ, даже если и преобладаетъ одна цифра, то она можетъ распредѣлиться по вертикальнымъ столбцамъ крайне непропорціонально, и такимъ образомъ нѣкоторые столбцы таблицы № 51 дали бы фальшивые максимумы. Главное, мы не можемъ здѣсь по нѣсколькимъ открытымъ уже цифрамъ періода возстановить всѣ остальныя, какъ мы это дѣлали съ предыдущими періодическими системами, ибо первичный текстъ представляетъ тоже нѣчто совершенно неизвѣстное. Можно еще болѣе затруднить раскрытіе, если самый періодъ *измѣнять періодически.* Напр., при второмъ наложеніи періода начинать его со второй цифры, т. е. укоротить его на 1 цифру; при третьемъ наложеніи начать съ третьей цифры и т. д.

Поэтому описываемую систему можно было бы, при извѣстныхъ предосторожностяхъ и при соблюденіи нѣкоторыхъ правилъ, считать близкой къ идеалу, если бы она была удобна для примѣненія. Но этого послѣдняго объ ней сказать нельзя. Составлять первую криптограмму, приготовить числовой періодъ (чѣмъ длиннѣе—тѣмъ хлопотливѣе), надписывать его и складывать, помнить, гдѣ остановились на ключѣ при остановкахъ и перерывахъ—все это дѣлаетъ эту систему весьма мало пріятной. Но для надежной записи, для памяти, небольшихъ текстовъ — адресовъ, паролей и т. д., при соблюденіи предосторожностей, о которыхъ рѣчь будетъ въ XVIII и XXI главахъ, эту систему можно считать достаточной.

Глава XV.

„КНИЖНЫЙ“ ШИФРЪ.

„Не радуйся, мой свѣтъ“,
—Ей крыса говоритъ въ отвѣтъ:
„И не надѣйся попустому!“

До сихъ поръ мы все имѣли дѣло съ такими системами, гдѣ либо *искусственно* составлялся опредѣленный, ограниченный, извѣстнымъ образомъ пронумерованный складъ буквъ, либо записанный цифрами текстъ подвергался искусственному измѣненію при помощи періодическаго извратителя. Мы видѣли, что второй типъ оказывается еще хуже перваго, какъ съ точки зрѣнія примѣненія, такъ и въ смыслѣ надежности. Главный же недостатокъ системъ перваго типа—бѣдность и нецѣлесообразность распредѣленія знаковъ.

Теперь мы займемся естественной системой, въ которой вмѣсто искусства выступаетъ природа. Ужъ давно было сказано, что

Блѣдно созданное нами
На домашнихъ алтаряхъ;
А творимое природой
Блещетъ въ утреннихъ лучахъ.

Здѣсь мы будемъ имѣть случай лишній разъ въ этомъ убѣдиться.

Правда, можетъ показаться страннымъ называть книгу произведеніемъ природы. Но въ извѣстномъ смыслѣ это допустимо. По сравненію съ тѣми чисто искусственными скопленіями буквъ, которыя мы встрѣчали на „развернутыхъ ключахъ“,—напечатанная въ книгѣ живая человѣческая рѣчь представляетъ *естественное* сочетаніе

звуковъ и буквъ, а прямоугольныя страницы, пронумерованныя, состоящія изъ горизонтальныхъ строчекъ, представляютъ превосходный *естественный* развернутый ключъ.

Способъ зашифровыванія, очевидно, не можетъ представлять никакихъ затрудненій. Для этого годится *всякій* напечатанный текстъ, ибо онъ всегда располагается строчками, прямоугольными страницами или столбцами: книги, брошюры, газеты. Очевидно, надо только условиться относительно названія книги, *изданія* ея и страницы. Затѣмъ каждая буква выразится дробью, гдѣ числитель обозначаетъ номеръ строчки, а знаменатель—мѣсто буквы на ней.

Изданіе книги необходимо заранѣе указывать, потому что въ разныхъ изданіяхъ разная нумерація страницъ, также различны размѣръ, строеніе и т. д. Поэтому нѣтъ возможности прочесть криптограмму, пользуясь другимъ изданіемъ.

Очевидно, нѣтъ никакой надобности ограничиваться при зашифровываніи одной страницей. Ничто не мѣшаетъ въ одномъ и томъ же письмѣ перескакивать съ одной страницы на другую. Надо только всякій разъ обозначать переходъ на другую страницу, а также на какую именно. Обыкновенно страница обозначается цѣлымъ числомъ. Напримѣръ:

$$16 \quad {}^{13}/_{25},\ {}^{1}/_{4},\ {}^{1}/_{15},\ {}^{10}/_{7},\ {}^{25}/_{3}\ldots\ {}^{4}/_{6},\quad 21 \quad {}^{17}/_{5},\ {}^{8}/_{3},\ {}^{6}/_{5}\ldots$$

Здѣсь начали шифровать по 16-ой страницѣ, а потомъ перешли на 21-ую.

Другіе обозначаютъ страницу и переходъ съ одной на другую *внутреннимъ* способомъ, незамѣтнымъ для непосвященнаго. Напр., 16 можно было бы условно изобразить въ видѣ дроби ${}^{3}/_{13}$, гдѣ сумма числителя и знаменателя указываетъ страницу, или какъ-нибудь иначе. Переходъ съ одной страницы на слѣдующую можно сигнализировать незамѣтно посредствомъ условнаго сочетанія буквъ, а то совсѣмъ просто посредствомъ ъ, который вообще не употребляется. Напр., въ фразѣ: „Намъ нужъен наборщъик"..., если ее зашифровать по книгѣ, читающій дважды натолкнется на призывъ перевернуть страницу.

Для облегченія шифрованія по книгѣ весьма цѣлесообразно пользоваться бумажной ленточкой. Приложивъ ее вертикально къ лѣвому краю страницы, наносятъ на ней нумерацію строчекъ; получается нѣчто въ родѣ измѣрительной ленты. Вмѣсто того, чтобы всякій разъ для каждой буквы отсчитывать строчки, мы прикладываемъ къ страницѣ ленту и на ней находимъ готовую нумерацію; при поворачиваніи страницъ ее приставляютъ къ слѣдующей. Не только получается огромное облегченіе, но и надежность сильно выигриваетъ, такъ какъ шифрующій при лентѣ свободно пользуется *всѣми* строчками страницы, тогда какъ безъ этого онъ, лѣнясь отсчитывать, довольствуется верхними. Буквы же на строчкахъ приходится отсчитывать. Можно бы и здѣсь приспособить горизонтальную ленту, но примѣненіе ея не дастъ большого выигрыша, ибо ее приходилось бы безпрерывно передвигать по страницѣ и налаживать.

Особенности системы. Громадныя преимущества этой системы бросаются сразу въ глаза. Количество знаковъ, которыми она располагаетъ, колоссально и далеко оставляетъ за собой всевозможныя искусственныя системы. Если даже ограничиваться одной страницей, то и тогда мы имѣемъ въ среднемъ до 2000 буквъ. Если же мѣнять страницы, то обыкновенная книга въ 20 листовъ дастъ до 600 тысячъ буквъ! Есть, значитъ, изъ чего выбирать. Въ этомъ послѣднемъ случаѣ шифръ, собственно, становится перемѣннозначнымъ, такъ какъ одинъ и тотъ же знакъ, напр., ${}^{13}/_{7}$, означаетъ на разныхъ страницахъ, а слѣдовательно, въ разныхъ мѣстахъ криптограммы разныя буквы. Но этого еще мало. Буквы въ книгѣ находятся въ естественной пропорціи, т. е. именно въ той, которая нужна для зашифрированія. Самая частая буква *о* въ такой книгѣ изъ 20 листовъ встрѣтится до 67000 разъ, а самая рѣдкая буква *ф* всего 60 разъ. Наконецъ, между знаками нѣтъ рѣшительно никакой математической или какой-либо другой связи, такъ что угадавъ даже цѣлыя фразы, мы не въ состояніи были бы добраться до остальныхъ знаковъ.

Что касается до примѣненія, то книжный шифръ относится къ разряду удобныхъ. Никакой таблицы, никакихъ предварительныхъ манипуляцій не нужно. Выбирать знаки, особенно съ помощью ленточки, дѣло легкое. Однимъ словомъ, если можно говорить объ идеалѣ, то таковымъ по всѣмъ признакамъ является разбираемая система.

Распознаваніе системы. Сообразить, что данный текстъ зашифрованъ по книгѣ— дѣло нетрудное. Во первыхъ, знаками обязательно служатъ дроби; во вто-

рыхъ, и числители и знаменатели могутъ быть и въ дѣйствительности бываютъ довольно высокія числа, такъ какъ число строкъ на страницѣ бываетъ въ среднемъ 35 – 40, а число буквъ въ строчкѣ можетъ доходить до 70. Смѣшеніе возможно либо съ многоклѣточнымъ простымъ квадратнымъ, въ которомъ ключъ превышаетъ 10 буквъ (см. гл. IV), либо съ „стихотворнымъ" шифромъ (гл. XVI). Однако, въ 1-омъ числитель рѣдко превышаетъ 20, такъ какъ обыкновенно не берутъ такихъ длинныхъ ключей (мы не встрѣчали на практикѣ ключей длиннѣе 16 буквъ); что до отличія отъ стихотворнаго, то оно указано будетъ въ слѣдующей главѣ.

Раскрытіе шифра. Не нужно много размышлять, чтобы понять всю безнадежность попытокъ расшифровать текстъ, гдѣ каждая буква можетъ имѣть отдѣльный знакъ, гдѣ между знаками нѣтъ никакой связи. Сколько ни сидѣть надъ криптограммой, изъ анализа ничего не удастся выжать. Нѣтъ сомнѣнія, что иногда удавалось и здѣсь добраться до смысла при помощи внутренняго анализа. Но это случалось лишь потому, что шифровка производилась самымъ возмутительно небрежнымъ образомъ: не только довольствовались одной страницей, но и на ней по лѣни ограничивались нѣсколькими верхними строками и близкими къ лѣвому краю буквами. Намъ извѣстенъ случай, когда корреспондентъ, чтобы не быть въ зависимости отъ книги, выписалъ себѣ изъ условной страницы верхнія 10 строкъ, да и изъ нихъ лишь лѣвыя половины. Другой заучилъ *наизусть* значенія буквъ, чтобы шифровать безъ книги—и можно себѣ представить, какъ скуденъ былъ запасъ знаковъ въ его памяти; *такой* книжный шифръ есть, конечно, одна лишь пародія. Однако, за такія извращенія система не можетъ быть отвѣтственна; шифровать здѣсь lege artis нисколько не затруднительно и для этого не требуется никакого умѣнья и пониманія; а во всѣхъ такихъ случаяхъ разгадка безнадежна.

Но если нельзя добраться до ключа внутреннимъ путемъ, то есть внѣшній. Въ противность искусственнымъ системамъ, въ которыхъ ключъ спрятанъ глубоко въ извилинахъ мозга, здѣсь онъ есть полнѣйшая реальность, которая первымъ дѣломъ бросается въ глаза при обыскахъ. Безъ условленной книги нельзя ни написать, ни прочесть письма; у корреспондента, поэтому, есть лишь 2 пути: либо держать книгу всегда при себѣ, въ дорогѣ же приходится по неволѣ возить ее съ собою, — либо въ другомъ мѣстѣ. Въ первомъ случаѣ она будетъ найдена у него при обыскѣ, во второмъ - приходится всякій разъ при отправленіи или для прочтенія письма ходить за книгой. Помимо того, что это затрудняетъ переписку, нѣтъ никакой гарантіи, что при такихъ частыхъ прогулкахъ не затащишь туда шпіона, результатомъ чего опять таки можетъ быть обыскъ и нахожденіе книги. Для жандармовъ достаточно лишь при обыскѣ записать заглавія и изданія найденныхъ книгъ, чтобы имѣть въ рукахъ ключъ къ разгадкѣ захваченныхъ какъ ранѣе, такъ и при обыскѣ шифрованныхъ документовъ. Если даже у А не было еще обыска, то онъ не можетъ быть гарантированъ, что не произведенъ уже обыскъ у кого-нибудь изъ его корреспондентовъ. Очень часто простое сравненіе списковъ книгъ, найденныхъ у нѣсколькихъ лицъ въ одномъ районѣ, сейчасъ же выдѣляетъ специфическую книгу, служившую ключомъ, такъ какъ она имѣется у каждаго. Я уже не говорю о томъ, что нѣкоторыя категоріи книгъ прямо сдѣлались въ этомъ отношеніи излюбленными—явленіе до такой степени частое, что нерѣдко можно подобрать книгу такимъ же образомъ, какъ подбираютъ обыкновенные ключи къ замку. Убѣдиться, что такая-то книга *не* подходитъ, въ особенности, если страница обозначена, дѣло 1-2 минутъ; если не обозначена, то нѣсколькихъ часовъ.

Нѣкоторые прибѣгаютъ при зашифровываніи по книгѣ къ фокусамъ, чтобы обмануть бюро: шифруютъ снизу вверхъ, справа налѣво, отступаютъ на нѣсколько строкъ отъ начала страницы и т. д. Все это основано на недоразумѣніи. Одно изъ двухъ: если книга остается жандармамъ неизвѣстной, то всѣ эти фокусы совершенно излишни; если же они до нея добрались, то ухищренія ни къ чему не приведутъ. Въ лучшемъ случаѣ потребуется для разгадки нѣсколько лишнихъ часовъ.

Заключеніе. Для дипломатовъ и посланниковъ, пользующихся и у себя на родинѣ и, въ силу экстерриторіальности, въ чужихъ странахъ совершенной безопасностью отъ обысковъ, для департамента полиціи и жандармскихъ управленій, вполнѣ обезпеченныхъ отъ непрошеннаго ночного посѣщенія со стороны революціонеровъ—лучшей системы при обмѣнѣ шифрованными „нотами" и депешами нельзя и придумать. Россійскимъ же революціонерамъ ее рекомендовать нельзя. Употреблять ее вполнѣ спокойно можно лишь при нѣкоторыхъ исключительно благопріятныхъ обстоятель-

ствахъ: напр., если одинъ корреспондентъ находится за-границей, а другой живетъ при библіотекѣ, гдѣ его книга исчезаетъ въ массѣ другихъ, или при такихъ условіяхъ, что на случай обыска книга можетъ быть уничтожена, и т. п. При этомъ необходимо во всякомъ случаѣ соблюдать извѣстныя предосторожности:

1) Страница, съ которой начинаютъ шифрованіе, должна быть условлена заранѣе. Обозначать ее тутъ же открыто нельзя;

2) Пользоваться надо многими страницами, переходя постепенно на слѣд.;

3) Сигналы для перехода должны быть обязательно внутренніе, т. е. незамѣтные извнѣ,—лучше всего при помощи буквъ;

4) Изъ спеціальныхъ „ухищреній" полезно прибѣгать къ такому: на каждой страницѣ начинать счетъ строкъ не съ первой, а съ заранѣе условленной, напр., съ восьмой. Ленту въ такомъ случаѣ готовятъ такъ: противъ первой строчки ставятъ черточку, а противъ условной (т. е. восьмой) единицу, а затѣмъ уже ведутъ послѣдовательную нумерацію. Это „усовершенствованіе" не требуетъ отъ шифрующаго ни единаго лишняго усилія или потери времени, а разгадку затрудняетъ.

Глава XVI.

СТИХОТВОРНЫЙ ШИФРЪ.

Ой, братцы, мало асъ;
Голубчики, немножко!

Народная пѣснь.

Предыдущую систему, превосходную самое по себѣ, пришлось забраковать исключительно потому, что ключъ въ его естественномъ матеріальномъ видѣ приходится постоянно держать по близости. Однако, есть полная возможность держать живую рѣчь и въ головѣ, куда добраться не найдено еще прямыхъ способовъ. Очевидно, тутъ не только требуется держать въ памяти текстъ, но необходимо еще, чтобы онъ располагался неизмѣннымъ образомъ, опредѣленными строчками, въ формѣ постоянно одинаковой, себѣ равной таблицы. Этому условію вполнѣ удовлетворяетъ стихотворная форма словесности. Стихи, съ одной стороны, легко запоминать наизусть безъ того, чтобы забывать отдѣльныя слова и ихъ *порядокъ*; съ другой стороны, каждая строчка вполнѣ опредѣлена, ограничена и даже всегда отмѣчается заглавной буквой. Однимъ словомъ, стихотвореніе какъ будто для того и существуетъ, чтобы рѣшить, наконецъ, трудный вопросъ о шифрѣ.

Чтобы пользоваться этой системой, очевидно достаточно корреспондентамъ условиться относительно выбора стихоренія. Послѣ этого самый способъ записыванія не представляетъ ничего особеннаго. Выписываемъ аккуратно условное стихотвореніе въ той формѣ, какъ оно обыкновенно печатается, нумеруемъ строчки и, выбравъ нужную букву, обозначаемъ ее дробью, гдѣ числителемъ служитъ номеръ строчки, а знаменателемъ мѣсто буквы на ней. Такъ напр., фраза: „Нам нужен наборщик", зашифрованная по баснѣ Крылова „Стрекоза и Муравей", можетъ быть изображена такъ: $^1/_8$, $^4/_2$, $^5/_3$, $^6/_1$, $^3/_6$, $^6/_6$, $^1/_{14}$, $^{10}/_1$, $^{10}/_{12}$, $^2/_7$, $^6/_{24}$, $^2/_4$, $^5/_5$, $^9/_7$, $^4/_6$, $^2/_5$.

Очевидно, что когда берутъ въ качествѣ ключа стихотвореніе иностраннаго поэта, то необходимо условиться и объ имени переводчика, иначе письмо можетъ остаться непрочитаннымъ, если получатель будетъ пользоваться другимъ переводомъ.

Особенности системы. Обыкновенное стихотвореніе содержитъ 30-40 строкъ по 20-25 буквъ въ среднемъ, что даетъ до 600-1000 буквъ въ совокупности. Напр., басня Крылова „Волкъ на псарнѣ" содержитъ 830 буквъ. Распредѣлены онѣ, какъ во всякой живой рѣчи, вполнѣ цѣлесообразно, въ надлежащей пропорціи; никакой связи между знаками нѣтъ. Общее количество знаковъ таково, что его вполнѣ хватаетъ на обыкновенную криптограмму, которая рѣдко превышаетъ 1000 буквъ; благодаря этому каждый знакъ приходится примѣнять не чаще 1-2 разъ. Контролировать такое планомѣрное, равномѣрное пользованіе всѣми знаками здѣсь очень легко, такъ

какъ стоитъ лишь всякую употребленную букву отчеркивать на выписанномъ текстѣ стихотворенія. Вообще примѣненіе этого шифра дѣло не хлопотливое: надо лишь потратить нѣкоторое время на выписку стихотворенія. Однимъ словомъ, тутъ мы, повидимому, обрѣли идеалъ, къ которому мы тщетно стремимся.

Распознаваніе системы. Смѣшать ее можно только съ многоклѣточнымъ квадратнымъ шифромъ и съ книжнымъ ключомъ. Отъ перваго ее отличить весьма легко: во 1-ыхъ, числители въ немъ всегда будутъ меньше, чѣмъ въ стихотвореніи, гдѣ число строкъ бываетъ 20-30-40; во 2-хъ, въ стихотвореніи, при сколько-нибудь правильной шифровкѣ, знаки или вовсе не повторяются, или повторяются равномѣрно. Въ квадратномъ же многіе повторяются часто, а многіе вовсе не встрѣчаются. Труднѣе отличить отъ книжнаго. Здѣсь часто можетъ выручить одинъ только предательскій знаменатель. Дѣло въ томъ, что въ книгѣ число буквъ въ строчкѣ колеблется въ предѣлахъ 40-70, между тѣмъ какъ въ стихотвореніяхъ онѣ значительно короче. Самые короткіе стихи — двухстопные ямбы или хореи — содержатъ всего 10-12 буквъ; самые длинные — шестистопные дактили (гекзаметры) — до 40 буквъ. Самая же частая форма — четырехъ или пятистопный ямбъ — даетъ 20-27 буквъ. Ясно, что стоитъ только разъ попасться большому знаменателю (выше, напр., 30) и мы діагносцируемъ „книгу". — Если при книжномъ шифрѣ мѣняютъ страницы, то могутъ часто повторяться одни и тѣ же знаки (что, конечно, не бѣда, само по себѣ), между тѣмъ какъ въ стихотвореніяхъ знаки попадаются равномѣрно. Внимательный глазъ много добудетъ въ смыслѣ діагноза „косвенныхъ уликъ" изъ изученія частоты дробей съ числителемъ 1 и 2 (объ этомъ ниже). Наконецъ, само собою разумѣется, если среди дробей попадаются вдругъ цѣлыя числа, то это сейчасъ показываетъ, что имѣемъ дѣло съ книгой, такъ какъ они обозначаютъ страницы.

Раскрытіе шифра. Итакъ, систему узнать нетрудно; значитъ ли это, что можно и раскрыть шифръ? Апріорно приходится рѣшить этотъ вопросъ отрицательно. Такая система, гдѣ знаки встрѣчаются равномѣрно, гдѣ нѣтъ между ними никакой внутренней связи — недоступна. Нельзя, конечно, отрицать, что въ дѣйствительности рѣдко примѣняютъ ее раціонально. Мы можемъ даже съ увѣренностью сказать, что никогда. Во всѣхъ случаяхъ, съ которыми намъ приходилось имѣть дѣло, мы ни разу не видѣли, какъ ни кратки были криптограммы, чтобы знаки встрѣчались однократно. При базисномъ способѣ записыванія это давало возможность раскрывать и такіе шифры, причемъ какое именно стихотвореніе служило ключомъ — оставалось неизвѣстнымъ. Одинъ разъ удалось даже и этого добиться, благодаря тому, что въ зашифрованномъ адресѣ распознано было слово „до востребованія", и слогъ „стре" былъ изображенъ знаками: $^{11}/_{1}$, $^{11}/_{2}$, $^{11}/_{3}$, $^{11}/_{4}$. Это показывало, что одиннадцатая строчка неизвѣстнаго стихотворенія начинается словомъ „Стре...". Вспомнили о словѣ „Стрекоза", а затѣмъ, естественно, и о баснѣ „Стрекоза и Муравей". Подобнаго рода крупные промахи, какъ многократное пользованіе одними и тѣми же *знаками*, или пользованіе рядомъ знаковъ, непосредственно слѣдующихъ одинъ за другимъ, объясняется исключительно лѣнью, легкомысліемъ, халатностью корреспондентовъ. Иной запоминаетъ только нѣсколько строкъ, другой хотя помнитъ все стихотвореніе, но лѣнится выписать его цѣликомъ и ограничивается верхними строфами. И сверхъ того, не желая затруднять себя отсчитываніемъ, беретъ тѣ буквы, которыя ближе къ лѣвому краю. Въ результатѣ выходитъ, что врядъ ли эксплуатируется даже десятая часть знаковъ, и самъ по себѣ безукоризненный и недоступный шифръ дѣлается сомнительнымъ. Но, повторяемъ, система не можетъ быть отвѣтственна за плохихъ ея послѣдователей, если только соблюденіе всѣхъ ея требованій практически легко выполнимо и не требуетъ большихъ жертвъ въ отношеніи усидчивости, терпѣнія, вниманія, времени. Здѣсь все это чрезвычайно облегчено.

И несмотря на такое внутреннее совершенство и неуязвимость стихотворнаго шифра, онъ такъ же мало является идеаломъ, какъ и всѣ предыдущіе, и мы такъ же далеки отъ цѣли, какъ были раньше. Намъ незачѣмъ ломать себѣ голову надъ внутреннимъ анализомъ криптограммы. Разъ мы констатировали, что имѣемъ дѣло со стихотвореніемъ, намъ нужно *подобрать* подходящее, что гораздо легче, чѣмъ можетъ показаться на первый взглядъ. Дѣло въ томъ, что число стихотвореній вообще не безконечно. Если исключить всѣ тѣ, которыя по своимъ малымъ размѣрамъ не годятся (напр. 4—15 строкъ), а также устарѣлыя, совершенно неизвѣстныя и т. п., то врядъ ли ихъ число окажется больше 20.000. Вообразите теперь, что изъ этихъ стихотвореній сдѣланъ большой альбомъ, гдѣ они расположены въ такомъ порядкѣ,

что съ самаго начала идутъ самыя извѣстныя стихотворенія, знакомыя каждому школьнику, а чѣмъ далѣе, тѣмъ все менѣе популярныя. При этомъ въ каждой категоріи они расположены еще по удобству своего запоминанія, или примѣненія: болѣе удобныя раньше, менѣе удобныя—послѣ. Если бы даже пришлось перебрать всѣ 20 тысячъ стихотвореній—случай невозможный, ибо часть придется исключить по одному тому, что по своей длинѣ или размѣру (число буквъ въ стихѣ) они меньше предполагаемаго,—то и тогда, считая по 1 минутѣ на каждую пробу, потребуется около 333 час. или 1 мѣсяцъ. Въ дѣйствительности же потребуется... полчаса или часъ. По самой сущности этой системы приходится выбирать, въ качествѣ ключей, такія стихотворенія, которыя общеизвѣстны. Вѣдь ихъ надо держать въ памяти, а революціонеру нѣтъ времени заучивать наизусть стихотворенія. Къ тому же ихъ надо знать въ совершенствѣ, не измѣняя и не переставляя словъ, не перепутывая строфъ и т. д. Если забыть стихотвореніе, то надо имѣть возможность возстановить его въ памяти, добывъ книгу, гдѣ оно напечатано; а легко найти эту книгу (у себя держать ее, конечно, нельзя) можно лишь тогда, когда данное стихотвореніе употребительно. Надо еще принять во вниманіе, что обыкновенно о ключѣ уславливаются письменно, а если и устно, то наскоро. Далѣе, корреспонденты безпрерывно мѣняются, ключъ переходитъ отъ одного къ другому. Часто корреспондента арестовываютъ, и „связи", въ видѣ адресовъ и шифровъ, достаются наслѣдникамъ въ формѣ краткихъ записей. Все это ведетъ неизбѣжно къ тому, что ключами выбираются первыя попавшіяся, извѣстныя обѣимъ сторонамъ, т. е. самыя избитыя стихотворенія. И дѣйствительно, во *всѣхъ* случаяхъ стихотворнаго ключа, съ которыми мы встрѣчались, „ключи" можно было найти въ любой христоматіи, ихъ знаетъ наизустъ любой школьникъ. Недаромъ „Искра" въ одномъ изъ своихъ номеровъ напоминаетъ, чтобы не брали для шифровъ „слишкомъ извѣстныхъ" стихотвореній. Совѣтъ этотъ хорошъ, хотя и недостаточно категорическій. Если уже брать стихотворенія, то *совсѣмъ* неизвѣстныя. Но совѣтъ этотъ во всякомъ случаѣ принадлежитъ къ числу платоническихъ, ибо революціонеры не станутъ разыскивать и зубрить невѣдомыя вирши. Послѣ всего сказаннаго вполнѣ понятно, что во всѣхъ случаяхъ стихотворнаго шифра ключи окажутся въ самыхъ первыхъ нумерахъ нашего гипотетическаго альбома и, слѣдовательно, ларчикъ откроется необыкновенно быстро.

Отмѣтимъ еще нѣкоторыя особенности разбираемой системы. Въ иныхъ стихотвореніяхъ болѣе рѣдкія буквы могутъ отсутствовать; напр., въ баснѣ „Стрекоза и Муравей" вовсе не встрѣчаются буквы *ф* и *щ**). Это, конечно, не бѣда, хотя въ записываніи адресовъ требуется совершенная точность; если отсутствіе этихъ буквъ замѣчено, то можно условиться относительно ихъ обозначенія. Во всякомъ случаѣ не слѣдуетъ, какъ дѣлаютъ нѣкоторые, помѣщать отсутствующую букву въ ея естественномъ видѣ посреди дробей, напр.: ...$^{4}/_{7}{}^{2}/_{12}$ф$^{4}/_{3}$... или ..$^{2}/_{4}{}^{5}/_{3}$щ$^{4}/_{6}{}^{2}/_{3}$...

Другую особенность представляютъ первыя буквы стиховъ. Въ книгахъ строки часто начинаются обломкомъ слова, благодаря тому, что оно не помѣстилось на предшествующей строкѣ и конецъ его „перенесенъ". Здѣсь же каждый стихъ начинается цѣлымъ словомъ. Чрезвычайно часто такими начальными словами являются союзы и предлоги; послѣдніе—либо самостоятельно, либо какъ передняя часть слова. Чаще всего встрѣчаются *въ, но, на, съ, къ, и, подъ, при, по* и т. д. Поэтому подавляющее большинство стиховъ начинается съ *и, в, п, н, с, к, о***). Это обстоятельство можетъ оказать услугу какъ при распознаваніи системы, такъ и при дешифрированіи. Поэтому первыми буквами надо поменьше пользоваться.

Заключеніе. Изъ сказаннаго ясно, что пользованіе этимъ шифромъ тогда только допустимо, когда выбранное стихотвореніе крайне рѣдкое, совершенно неизвѣстное (еще лучше нигдѣ не напечатанное). Но такое требованіе, конечно, сильно уменьшаетъ подвижность этого шифра, легкость передачи его отъ одного корреспондента другому. Затѣмъ при широкой перепискѣ запоминать нѣсколько такихъ стихотвореній—бремя не малое. При этомъ нужно: 1) пользоваться всѣми знаками, отчер-

---

*) Намъ, поэтому, пришлось во взятомъ выше образчикѣ „намъ нуженъ наборщикъ" замѣнить отсутствующее *щ* посредствомъ *ш*.

**) Въ 1000 стихахъ изъ числа начальныхъ буквъ оказалось: 124—*и*, 116—*в*, 84—*п*, 72—*н*, 71—*с*, 57—*о*, 51—*т*, *к* и т. д. Первыя 5 буквъ охватываютъ, такимъ образомъ, болѣе $^{2}/_{5}$ *общаго* количества. Второй буквой часто служитъ неупотребительный *ъ* (въ, съ, къ).

кивая ихъ для контроля, по мѣрѣ утилизаціи; 2) условиться относительно отсутствующихъ рѣдкихъ буквъ; 3) меньше пользоваться первыми буквами стиховъ; 4) полезно начать счетъ строчекъ не съ первой, а съ другой, напр. пятой, восьмой и т. п., хотя это уменьшаетъ число знаковъ; или же условно перемѣстить нѣсколько строфъ такъ, чтобы на мѣсто первой очутилась какая-нибудь другая. Это затрудняетъ производство „пробъ" и удлиняетъ періодъ времени, потребный для раскрытія.

Во всякомъ случаѣ объ „идеалѣ" говорить тутъ не приходится. „Еще не въ присгани нашъ флотъ!"

Глава XVII.

УХИЩРЕНІЯ или ПАЛЛІАТИВЫ.

Неувѣренность въ существующихъ системахъ, хотя и недостаточно мотивированная, побуждала многихъ не ограничиваться извѣстнымъ типомъ, а ввести „улучшенія". Нѣкоторыя изъ нихъ крайне наивны и разсчитаны только на то, что „тамъ" не догадаются. Другія таковы, что улучшая въ одномъ отношеніи, ухудшаютъ въ другомъ и тѣмъ еще сильнѣе подчеркиваютъ нераціональность основного типа. Иныя же заслуживаютъ вниманія. Мы разберемъ здѣсь нѣкоторыя изъ тѣхъ, съ которыми мы встрѣчались на практикѣ.

1) Въ одной организаціи долго употреблялся для самыхъ конспиративныхъ сообщеній *простой* квадратный шифръ съ такимъ „усовершенствованіемъ": десятый вертикальный столбецъ (стало быть знаки 10, 20, 30 и т. д.) отрѣзывался, а отрѣзанные знаки приравнивались соотвѣтственно знакамъ десятаго горизонтальнаго ряда (01, 02), такъ что 10=01; 20=02; 30=03 и т. д. Вотъ и все, ни больше, ни меньше! Эта тришкинская операція, разумѣется, ни на іоту не улучшала никуда негоднаго шифра. Зато, когда одному товарищу пришлось по необходимости попытаться расшифровать письмо, написанное по этой „улучшенной" системѣ, то это было продѣлано въ какія-нибудь 15 минутъ. Спрашивается, кого же этими благоглупостями благообмануть хотятъ?

2) При употребленіи книжнаго и стихотворнаго шифра, для того, чтобы сбить жандармовъ, нѣкоторые уславливаются вставлять фальшивыя дроби на опредѣленныхъ мѣстахъ, напр., черезъ каждые 4 знака. Это, конечно, не то, что разобранный нами въ VI главѣ прерывистый квадратный шифръ съ фиктивными цифрами; тамъ цифры вставлялись стихійно, какъ богъ на душу положитъ; здѣсь любыя фиктивныя дроби ставятся на строго опредѣленныхъ мѣстахъ. Но выигрышъ отъ этого очень маленькій. Прежде всего вообще смѣшно выѣзжать на такихъ дѣтскихъ элементарныхъ ухищреніяхъ, гдѣ вся цѣль заключается въ томъ, чтобы обмануть, весь разсчетъ построенъ на томъ, что „тѣ" не сообразятъ; трудно себѣ представить, чтобы столь примитивные пріемы не были извѣстны „бюро". Но если бы этотъ фокусъ даже и не былъ извѣстенъ, то странно думать, что разъ книга или стихотвореніе угаданы, или если при производствѣ пробы дошли до дѣйствительнаго ключа, то фиктивные знаки спасутъ. Положимъ, что послѣ того, какъ мы перепробовали нѣсколько стихотвореній и получили совершенно дикія сочетанія звуковъ, у насъ сложилась такая группа буквъ: „полубчили". Самый неопытный человѣкъ немедленно остановится на такомъ сочетаніи и сейчасъ же догадается, что буква *б* здѣсь лишняя, а надо читать „получили". Совершенно не достигая цѣли, это „улучшеніе" въ то же время удлиняетъ текстъ и отнимаетъ много времени и вниманія у обоихъ корреспондентовъ.

3) Одинъ разъ мы встрѣтились съ попыткой усовершенствовать сложный квадратный шифръ посредствомъ введенія и вертикальнаго распредѣлителя. Вмѣсто того, чтобы пронумеровать горизонтальные ряды въ послѣдовательномъ порядкѣ 1, 2, 3 и т. д., мы нумеруемъ ихъ иначе, напр.: 4, 7, 2, 3 и т. д. Это, безспорно, улучшеніе, но спасаетъ ли оно? Вѣдь слабая сторона квадратнаго шифра—нахожденіе въ одномъ ряду десятибуквеннаго отдѣла азбуки — этой реформой не затрагивается. Тотъ или другой порядокъ горизонтальныхъ рядовъ зависитъ исключительно отъ порядка

буквъ въ ключѣ. Введеніе вертикальнаго распредѣлителя приведетъ лишь къ тому, что мы опредѣлимъ, быть можетъ, лишь *буквы* ключа, а не самый ключъ, и что нельзя будетъ по нѣкоторымъ найденнымъ уже буквамъ ключа отгадать остальныя.

4) Намъ пришлось встрѣтиться со случаемъ сложнаго квадратнаго шифра съ *двумя* ключами (таблица № 53). Одинъ писался подъ цифрой *1* распредѣлителя, другой (собственно говоря, тотъ же ключъ, но онъ шелъ снизу вверхъ) — подъ цифрой *6*. Остальныя цифры распредѣлителя отъ 1 до 5 включительно выполнялись отъ перваго ключа, а отъ 6 до 0 отъ второго. Это — значительное улучшеніе. Въ каждомъ горизонтальномъ ряду уже не десятибуквенный участокъ азбуки, а 2 пятибуквенныхъ, поэтому и разгадка сильно затрудняется. Но все же это лишь палліативъ, уменьшающій одинъ недостатокъ, но совсѣмъ не затрагивающій другой стороны — плохого количественнаго распредѣленія знаковъ. А оно можетъ здѣсь, наоборотъ, даже ухудшиться, ибо если одинъ ключъ и трудно подобрать такой, чтобы онъ далъ сносную пропорцію буквъ, то съ двумя еще труднѣе сладить. Чтобы убѣдиться въ этомъ, можно сравнить таблицу 53, гдѣ ключомъ служитъ „начальникъ“ (распредѣлителемъ тоже это слово) съ табл. № 12 (см. стр. 31), гдѣ имѣется всего одинъ ключъ „начальникъ“. Оказывается, напр., что *и* встрѣчается всего два раза (въ табл. № 12 – 3 раза), *е, ж, з* ни разу (въ табл. № 12 — по 2 раза).

Таблица № 53.

	1	2	3	4	5	6	7	8	9	0
	6	1	8	2	5	0	7	3	4	9
1	*ъ*	*н*	ь	о	с	э	ы	п	р	ѣ
2	*к*	*а*	м	б	д	о	л	в	г	н
3	*и*	*ч*	й	щ	ы	л	і	щ	ъ	к
4	*н*	*а*	п	б	д	с	о	в	г	р
5	*ь*	*л*	э	м	п	я	ѣ	н	о	ю
6	*л*	*ь*	н	ѣ	я	п	м	э	ю	о
7	*а*	*н*	в	о	с	д	б	п	р	г
8	*ч*	*и*	щ	і	л	ы	ш	й	к	ъ
9	*а*	*к*	в	л	о	д	б	м	н	г
0	*н*	*ъ*	п	ы	э	с	о	ь	ѣ	р

5) Приходилось намъ также имѣть дѣло со сложнымъ квадратнымъ шифромъ, въ которомъ вмѣсто одного горизонтальнаго распредѣлителя имѣется ихъ нѣсколько (см. табл. № 54). Чтобы не брать нѣсколькихъ ключей-распредѣлителей, можно взять условную фразу, въ которомъ отдѣляемъ сперва 10 буквъ, потомъ еще 10 буквъ и т. д. (смотря по тому, сколько желаютъ взять распредѣлителей). Положимъ, что условная фраза: „Намъ нуженъ наборщикъ, нѣтъ ли подходящаго“, а распредѣлителей три. Выписываемъ фразу, отдѣляемъ 3 грани по 10 буквъ и въ каждой пронумеровываемъ буквы, какъ это обыкновенно дѣлается для распредѣлителей:

Н а м ъ н у ж е н ъ | н а б о р щ и к ъ н | ѣ т ъ л и п о д х о |
5 1 4 9 6 8 3 2 7 0 | 5 1 2 7 8 9 3 4 0 6 | 0 7 9 3 2 6 4 1 8 5 |

Получаемъ такимъ образомъ три распредѣлительныхъ числа. Положимъ, что условились писать первое наверху, второе послѣ третьяго ряда, а третье послѣ седьмого. Тогда, составивъ развернутый ключъ („начальникъ“) по „вторичному“ способу, вписываемъ нашихъ распредѣлителей въ указанныхъ мѣстахъ (табл. № [illegible]). Такимъ образомъ первые и послѣдніе но сеч[illegible] и средніе четыре составлены по разспособѣ; нь[illegible]чуламъ; напр., въ третьемъ вертелѣпость, без[illegible]тбцѣ слѣва буква *п* выражается 14, *в* — 4[illegible], *д* — 89, тогда какъ при одномъ верхнемъ распредѣлителѣ, онѣ бы обозначались: 14, 44, 84.

Таблица № 54.

	5	1	4	9	6	8	3	2	7	0
1	н	о	п	р	с	т	у	ф	х	ц
2	а	б	в.	г	д	е	ж	з	и	і
3	ч	ш	щ	ъ	ы	ь	ѣ	э	ю	я
	5	1	2	7	8	9	3	4	0	6
4	а	б	в	г	д	е	ж	з	и	і
5	л	м	н	о	п	р	с	т	у	ф
6	ь	ѣ	э	ю	я	а	б	в	г	д
7	н	о	п	р	с	т	у	ф	х	ц
	0	7	9	3	2	6	4	1	8	5
8	и	і	й	к	л	м	н	о	п	р
9	к	л	м	н	о	п	р	с	т	у
0	ъ	ы	ь	ѣ	э	ю	я	а	б	в

Благодаря такому усложненію, мы, узнавъ отношеніе двухъ какихъ-нибудь столбцовъ для одного ряда, ужъ не можемъ переносить его на всѣ остальные ряды, какъ это мы дѣлали въ V главѣ. Это — большое улучшеніе, но оно не уничтожаетъ основного недостатка квадратнаго шифра — нецѣлесообразнаго распредѣленія буквъ и, кромѣ того, специфическаго

состава буквъ въ каждомъ горизонтальномъ ряду. Повышается лишь минимумъ текста для разгадки—больше ничего.

6) Вмѣсто того, чтобы распредѣлителей размѣстить такъ, какъ на табл. № 54, можно ихъ помѣстить всѣ сверху и затѣмъ начать шифровать по первому распредѣлителю, потомъ перейти ко второму, затѣмъ къ третьему, наконецъ, опять вернуться къ первому распредѣлителю и т. д. (табл. № 55). Легко видѣть, что это не что иное, какъ множественный квадратный шифръ, описанный въ VII главѣ. Разница здѣсь только въ томъ, что тамъ составлялись нѣсколько таблицъ по разнымъ ключамъ, здѣсь же лишь одна таблица. Эта разница облегчаетъ пользованіе системой, ибо на составленіе одной таблицы требуется меньше времени, чѣмъ на составленіе нѣсколькихъ. Зато разгадка здѣсь тоже можетъ быть легче.

Таблица № 55.

III.	0	7	9	3	2	6	4	1	8	5
II.	5	1	2	7	8	9	3	4	0	6
I.	5	1	4	9	6	8	3	2	7	0
1	н	о	п	р	с	т	у	ф	х	ц
2	а	б	в		и т. д.					

7) Можно еще попытаться измѣнить порядокъ буквъ въ алфавитѣ, т. е. вмѣсто сложившагося порядка взять искусственный, условный. Для этого можно воспользоваться, напр., единозначнымъ парнымъ ключомъ:

ц ы р ю л ь п и к ъ х у д о щ а в
б г е ж з і й м п с т ф ч щ ѣ э я

Въ обоихъ рядахъ вмѣстѣ заключаются всѣ 34 буквы алфавита, и вотъ будемъ держаться того порядка, въ которомъ идутъ буквы сперва въ верхнемъ ряду, потомъ въ нижнемъ. На таблицѣ № 56 развернутъ ключъ „Хвощинская" по простой квадратной системѣ, причемъ буквы въ рядахъ идутъ въ вышеупомянутомъ искусственномъ порядкѣ. Хотя это усовершенствованіе затрудняетъ въ одномъ отношеніи разгадку, зато въ другомъ оно облегчаетъ, ибо пропорція буквъ получается еще менѣе выгодной, чѣмъ раньше. Напр., буквы: *с, т, р, л* встрѣчаются всего по 1 разу; зато *и, б,*—по 6 разъ.

Таблица № 56.

	1	2	3	4	5	6	7	8	9	0
1	х	у	д	о	щ	а	в	б	г	е
2	в	б	г	е	ж	з	і	й	м	п
3	о	щ	а	в	б	г	е	ж	з	і
4	щ	а	в	б	г	е	ж	з	і	й
5	и	к	ъ	х	у	д	о	щ	а	в
6	н	и	к	ъ	х	у	д	о	щ	а
7	с	т	ф	ч	ш	ѣ	э	я	ц	ы
8	к	ъ	х	у	д	о	щ	а	в	б
9	а	в	б	г	е	ж	з	і	й	м
0	я	ц	ы	р	ю	л	ь	п	и	к

8) Огромное распространеніе въ одной организаціи имѣлъ шифръ, построенный, какъ на базисѣ, на единозначномъ. При помощи остроумнаго разсчета буквы превращались въ цифры и затѣмъ вводились еще нѣкоторыя улучшенія и надстройки. Онъ былъ чрезвычайно удобенъ для употребленія и изобрѣтателямъ казался образцовымъ. За всѣмъ тѣмъ, если посудить да посмотрѣть, оказывается, что тамъ всего на всего штукъ 40 знаковъ—и это въ постояннозначной системѣ! Можно судить, насколько такая система прочна.

Этимъ мы закончимъ обзоръ частныхъ улучшеній. Конечно, описанныя нѣсколько улучшенія можно и комбинировать; напр., номера 3, 5 и 7, или 3 и 4 и т. д. фикгадка при этомъ затрудняется, но шифръ становится все менѣе практ- нѣсколько за сложности. Хорошаго, т. е. удобнаго и безусловно надежнаго шифръ сложилась путемъ не добьемся. здѣсь

Глава XVIII.

ОАЗИСНЫЙ И СПЛОШНОЙ СПОСОБЪ ЗАШИФРОВЫВАНІЯ.

Всѣ примѣрныя криптограммы, которыя мы разбирали въ предыдущихъ главахъ, представляли собой сплошной зашифрованный участокъ, безъ всякой посторонней примѣси: безъ раздѣленія словъ, безъ знаковъ препинанія, безъ перерывовъ, безъ побочныхъ вставокъ—буквенныхъ или числовыхъ, безъ подчеркиванія и, наконецъ, безъ всякой связи съ какимъ-либо контекстомъ, т. е. незашифрованными фразами; за исключеніемъ лишь XII главы, гдѣ криптограмма представляла 6 отрывковъ, во всѣхъ остальныхъ былъ единый, одиночный, самодовлѣющій участокъ. Такія письма на практикѣ бываютъ, однако, чрезвычайно рѣдки, врядъ ли 10%. Громадное большинство шифрованныхъ писемъ, которыми обмѣниваются у насъ революціонныя организаціи и отдѣльныя лица, состоятъ изъ перемежающихся между собою незашифрованныхъ и зашифрованныхъ участковъ, фразъ, частей предложенія и отдѣльныхъ словъ; встрѣчаются сокращенія, подчеркиванія, всевозможныя вставки, знаки препинанія: двоеточіе, скобки, ковычки, вопросительные и восклицательные знаки, красныя строки, во-1-хъ, во-2-хъ и т. п. роскошь, приличествующая лишь письмамъ незашифрованнымъ. Пишутъ, напримѣръ, такъ: „Вышлите мнѣ по извѣстному вамъ адресу немедленно *50* 639128. 7421425431268324414426 5435 (№ 1). Непремѣнно, здѣсь большая потребность". Зашифрованный участокъ означаетъ: „50 экз. рабочей газеты № 1".

Корреспондентъ шифруетъ лишь тѣ слова или фразы, которыя онъ считаетъ нужнымъ сдѣлать недоступными для жандармовъ на случай, еслибы имъ попало въ руки письмо. Нетрудно понять мотивъ, заставляющій его поступать такимъ образомъ. Писать и разбирать шифрованныя письма—дѣло не очень интересное и пріятное; оно отнимаетъ очень много времени, которымъ далеко не всегда располагаешь въ достаточномъ количествѣ. Къ тому же часто приходится писать спѣшно. Между тѣмъ любое письмо содержитъ тысячи буквъ и перевести его на шифрованный языкъ цѣликомъ—слишкомъ долгая работа. Да и получатель не разъ энергично выругается, добывая съ трудомъ, какъ изъ дегтя, тягучія фразы въ родѣ такой напримѣръ: „Мнѣ вполнѣ понятно неудовольствіе, которое вы проявляете по поводу того, что я такъ долго не отвѣчалъ на вашъ вопросъ, но войдите и въ наше положеніе, и т. д., и т. д.".

Неудивительно поэтому, что выработалась привычка шифровать письма не сплошь, а *оазисно*, т. е. отдѣльными участками.

На первый взглядъ, кажется, что оно даже и надежнѣе. Мы уже много разъ убѣждались, что чѣмъ больше зашифрованный текстъ, тѣмъ ярче проявляются законы фонетики и системы, и тѣмъ быстрѣе производится раскрытіе. Оазиснымъ же способомъ мы достигаемъ того, что изъ многихъ сотенъ или тысячъ буквъ письма зашифровывается лишь малая часть. Напр., во взятой нами для образца фразѣ, если бы ее зашифровать сплошь, оказались бы 123 буквы, а въ дѣйствительности зашифрованныхъ всего 16!

Но такой разсчетъ будетъ въ высшей степени неправильный. Прямо невозможно себѣ представить, какъ поразительно облегчается разгадка шифра при такомъ способѣ; никакія выраженія не будутъ достаточно сильными, чтобы заклеймить всю нелѣпость, безсмысленность, преступность обезопашивать такимъ образомъ важныя тайны.

Тутъ незачѣмъ прибѣгать ни къ какимъ выкладкамъ, подсчетамъ и хитроумнымъ соображеніямъ, которыя оказывались необходимыми при разборѣ сплошныхъ криптограммъ. Передъ нами не глухая, унылая, однообразная тайга цифръ безъ всякаго просвѣта, безъ всякой внѣшней путеводной нити, а пестрая, живая смѣсь фразъ, словъ, перемежающихся съ группами цифръ; множество зашифрованныхъ оазисовъ, которые глазъ можетъ сравнивать между собою, ставить въ связь съ контекстомъ, стараться *отгадать*. Въ томъ то и все дѣло, что здѣсь имѣется широкое поле для непосредственнаго отгадыванія буквъ, словъ, фразъ, а слѣдовательно, во всѣхъ безъ исключенія системахъ (кромѣ естественныхъ), и для рѣшенія всей задачи *).

---

*) О томъ, какое громадное облегченіе для *распознаванія системы* имѣетъ

Приходится отдать полную справедливость необычайной предупредительности и любезности нашихъ корреспондентовъ по отношенію къ „бюро" Департамента Полиціи; они какъ будто нарочно стараются изо всѣхъ силъ не долго его томить и облегчить его работу до послѣдней степени. Пишущій нисколько не задумывается о томъ, что въ каждой строчкѣ онъ оставляетъ на свою собственную погибель лазейки для раскрытія. Въ вышеприведенномъ примѣрѣ оазисной фразы добраться до смысла зашифрованнаго оазиса не составитъ никакого рѣшительно труда, ибо первое слово сейчасъ же отгадывается.

„Вышлите *50* 639128" — сейчасъ же наводитъ на мысль объ „экз", тѣмъ болѣе, что немного дальше въ скобкахъ фигурируетъ (№ 1). Вообще, разъ въ криптограммѣ встрѣчается отдѣльно стоящее или подчеркнутое небольшое число, то тутъ сейчасъ же заподазривается либо обозначеніе числа экземпляровъ, либо номеръ дома, квартиры, либо число людей (арестованныхъ и т. п.). Одно письмо, зашифрованное по простому квадратному шифру, удалось расшифровать (однимъ изъ товарищей — по необходимости) въ четверть часа по такой фразѣ: „ 10. 91. долженъ на это обязательно отозваться", такъ какъ изъ связи съ контекстомъ ясно видно было, что инціалы относятся къ Ц. К. (Центральный Комитетъ). Другое письмо было при такихъ же условіяхъ разобрано по фразѣ: „Здѣсь образовалась новая 2474599641. Выпустила листокъ". Нужно быть олухомъ, чтобы не догадаться сейчасъ же, что оазисъ означаетъ „група". Курьезно, что такъ какъ шифръ въ этомъ послѣднемъ случаѣ былъ простой квадратный изъ 9×10, то угаданное слово дало моментально 50 знаковъ, т. е. $^5/_9$ всѣхъ обозначеній!

Въ третьемъ письмѣ въ единичномъ *сплошномъ* текстѣ находилось въ серединѣ *двоеточіе*; это естественно навело на мысль, что передъ нимъ находится слово „адресъ", что вполнѣ подтвердилось.

Въ четвертомъ случаѣ тоже въ сплошномъ текстѣ замѣчено было подчеркнутое *17.6*, означавшее, очевидно, номеръ дома и квартиры; отсюда вывели, что предыдущее слово означаетъ названіе улицы и оканчивается поэтому на *...ая*, а вѣроятнѣе всего и на *...ская*, ибо большинство улицъ носятъ названія съ такимъ окончаніемъ. Это оправдалось и оказалось достаточнымъ для раскрытія.

Пятый, зашифровывая адресъ, ставитъ въ скобкахъ въ концѣ: (45516507438481); опытный глазъ, принимая во вниманіе мѣсто этой группы и количество въ ней буквъ, сейчасъ же сообразитъ, что это значитъ: *(для явки)*. Шестой такимъ же образомъ шифруетъ въ скобкахъ: „въ двухъ конвертахъ".

Письмо седьмого было разобрано потому, что оно начиналось въ высшей степени шаблонной фразой „Письмо получено". На мысль объ этомъ навело то, что первый и седьмой знаки были тождественные *(п)*. Отсюда, между прочимъ, понятна необходимость избѣгать шаблонныхъ фразъ въ началѣ письма.

Есть и такіе мудрецы, которые не сливаютъ даже вмѣстѣ словъ, а шифруютъ ихъ раздѣльно.

Какъ наглядный образчикъ легкости раскрывать оазисные тексты, помѣщаемъ здѣсь *безъ всякихъ измѣненій* письмо, полученное нашимъ товарищемъ отъ одного виднаго члена крупной русской организаціи. Нашъ товарищъ остался недоволенъ полученнымъ отъ послѣдняго шифрованнымъ письмомъ и сообщилъ ему, что такъ писать нельзя, что его письма легко расшифровать и безъ ключа. Тотъ усомнился и отвѣтилъ, что если *хорошо* шифровать, то, по его мнѣнію, разгадка невозможна (система была сложная квадратная); для доказательства онъ предложилъ разобрать „задачу", которую мы приводимъ на табл. № 57 въ подлинномъ ея видѣ съ сохраненіемъ даже размѣровъ строчекъ. Получившій задачу товарищъ разобралъ ее въ теченіе двухъ часовъ, догадавшись, что послѣднія два слова означаютъ „поживемъ увидимъ".

Повторяю, тотъ, кто составитъ себѣ мнѣніе о доступности нашихъ шифровъ исключительно по тѣмъ примѣрнымъ сплошнымъ криптограммамъ, которыя мы разбирали въ предыдущихъ главахъ, не будетъ имѣть никакого истиннаго представленія о легкости раскрытія тѣхъ конкретныхъ, реальныхъ писемъ, которыя въ дѣйствительности циркулируютъ между революціонерами, попадаютъ время отъ времени въ руки „бюро" и подвергаются его разбору. Даже болѣе трудныя и замысловатыя изъ разо-

---

множественность зашифрованныхъ отрывковъ, мы уже говорили раньше, при разборѣ прерывистаго квадратнаго, слитныхъ періодическихъ и другихъ. Здѣсь же мы говоримъ исключительно о раскрытіи шифра.

бранныхъ системъ, какъ сложный квадратный, множественный квадратный, вторичный слитный, разрѣшаются необыкновенно быстро при оазисномъ способѣ. Лишь на естественныя системы его вліяніе ограниченное: отгаданная цѣлая фраза, при правильной шифровкѣ, не должна дать никакихъ нитей для разбора остальныхъ участковъ. Догадливость имѣетъ такія широкія, растяжимыя границы, что тутъ возможны самые невѣроятные сюрпризы: „оазисность“ же даетъ благодарную почву для ея проявленія.

Таблица № 57.

Если 40332141464860527120133653545683417 0
89, то придется предложить 4011747579
84867758218273352919858382 10. Я одна-
ко думаю, что вамъ не 4049474120
36538242798758919811154164 своихъ
89291349. А впрочемъ 50794463101369
224072686388.

Какъ же, однако, шифровать письма? Неужели сплошь отъ начала до конца? Но это прямо невыгодно съ точки зрѣнія той же надежности, потому что легкость раскрытія, при прочихъ равныхъ условіяхъ, прямо пропорціональна количеству зашифрованныхъ буквъ. А съ точки зрѣнія практики это немыслимо, ибо сдѣлало бы переписку, по продолжительности и скукѣ, адской работой. Ясно, что между Сциллой и Харибдой надо найти какой-нибудь средній выходъ.

Прежде всего надо отмѣтить себѣ, что всякое письмо заключаетъ въ себѣ и такія извѣстія, которыя могутъ безъ вреда быть прочитаны жандармами, и секретныя сообщенія, конспиративныя свѣдѣнія, которыя никоимъ образомъ не должны стать имъ извѣстными. Къ первымъ относятся проявленія революціонной борьбы—демонстраціи, стачки, волненія, состояніе періодической и другой печати, т. е. все то, что могло бы появиться въ нелегальной прессѣ; также списки арестованныхъ, содержаніе допросовъ, свѣдѣнія о томъ, что найдено при обыскахъ и т. д. Конспиративнымъ является все то, открытіе чего можетъ принести хотя бы самый отдаленный вредъ движенію или какому-нибудь лицу.

Пишущій долженъ выработать себѣ привычку отдѣльно выписывать все то, чего незачѣмъ (а, значитъ, и не слѣдуетъ) шифровать. Все же конспиративное надо собрать вмѣстѣ; оно должно быть формулировано кратко, сжато, безъ вводныхъ словъ и разглагольствованій; слова надо предпочитать тѣ, что покороче: вмѣсто „сегодня“—„нынѣ“, вмѣсто „отправляться“—„ѣхать“, „арестованъ“—„взятъ“, „прокламаціи“—„листки“ и т. п. Полезно писать на „ты“, хотя бы и незнакомому человѣку: это значительно сокращаетъ многія слова: „пиши“, вмѣсто „пишите“ и т. п. Небезполезно также сокращать длинныя слова, но, разумѣется, никакихъ точекъ при этомъ ставить не слѣдуетъ, напр.: „Морскаяулдвадцатьтриквпятая“. Весь этотъ отдѣлъ долженъ представлять одну сплошную криптограмму. Никакихъ знаковъ препинанія, подчеркиваній красныхъ строкъ; числа надо писать прописью, стараться не заканчивать словъ къ концу строкъ. Таковъ идеалъ, къ которому надо стремиться.

Въ дѣйствительности, не всегда оказывается возможнымъ свести все къ *одному* зашифрованному отрывку: часто матеріалъ письма развивается у корреспондента во время процесса писанія, что исключаетъ возможность предварительной классификаціи его на двѣ категоріи. Въ этомъ случаѣ зашифрованныя сообщенія будутъ перемежаться съ записанными просто, криптограмма выйдетъ не единичной, а множественной, но она во всякомъ случаѣ должна остаться сплошной въ томъ смыслѣ, что отдѣльныя фразы, представляющія самостоятельное цѣлое, должны быть зашифрованы сплошь. Никоимъ образомъ нельзя зашифровывать отдѣльныя *части* предложенія. Записанная языкомъ цифръ фраза не должна быть ничѣмъ рѣшительно связана съ предыдущими и послѣдующими „открытыми“ фразами — ни въ грамматическомъ отношеніи, ни по смыслу. Напр., такое расположеніе свѣдѣній допустимо: „Арестовано 20 человѣкъ *къ вамъ ѣдетъ Михаилъ* вышелъ № 5 Жизни“. Напечатанная курсивомъ средняя фраза, которая должна быть изображена посредствомъ шифра, ничѣмъ не связана съ сосѣдними, и потому о ея смыслѣ догадаться невозможно. Вредная сторона такой формы заключается лишь въ томъ, что 1) облегчается распознаваніе

системы и 2) въ распоряженіи „бюро“ имѣется много началъ и концовъ фразъ, т. е. больше точекъ приложенія для угаданныхъ или предполагаемыхъ буквъ.

Приводимъ здѣсь примѣрный образчикъ нелегальнаго письма, гдѣ факты не систематизированы, а записаны такъ, какъ припоминались во время писанія, курсисомъ обозначены тѣ фразы, которыя обязательно должны быть зашифрованы.

„Оба ваши письма получены. 30 апрѣля были аресты. *Взяты Алексѣй, Андрей и Вѣра*, рабочіе Петровъ и Долгушенко, статистикъ Миклашевскій и ветеринаръ Брянцевъ, еще нѣсколько человѣкъ, фамиліи коихъ неизвѣстны. У Брянцева найдено около десяти брошюръ и взята ремингтонка, у остальныхъ ничего. *Литературу получилъ, очень нравится. Пришлите еще 2 пуда. Завтра вышлю 200 рублей по старому адресу. Сюда пишите по новому, Фундуклеевская 20, кв. 5, Александру Бугучеву.* Здѣсь уже 2 недѣли продолжается стачка на механическомъ заводѣ Иванченко, 1500 чел. Требуютъ сокращенія рабочаго дня до $10^1/_2$ час. *Нуждаются въ деньгахъ.* По поводу стачки успѣшно распространены листки, 5000 шт. *Въ концѣ іюня васъ посѣтитъ членъ здѣшняго Комитета, явится по данному адресу. Пароль: покончена ли черновая работа? Отвѣтить: спѣшить некуда.* Освобожденъ подъ надзоръ полиціи студ. Мылинъ. Вышелъ № 35 Искры, № 30 Arbeiterstimme, № 3 Краснаго Знамени“.

Всѣ курсивныя мѣста должны быть собраны вмѣстѣ. Фраза: „Взяты Алексѣй, Андрей и Вѣра“ никоимъ образомъ не должна быть оставлена на своемъ мѣстѣ, ибо она стоитъ въ тѣснѣйшей связи съ окружающимъ текстомъ. Тоже самое и о фразѣ „нуждаются въ деньгахъ“. Остальные два курсивные участка могли бы безъ особеннаго вреда остаться на своихъ мѣстахъ. При зашифровываніи въ отношеніи чиселъ, сокращеній и проч. должны быть соблюдаемы сдѣланныя выше указанія.

Глава XIX.

ВЫВОДЫ.

Подъ грозной броней ты не вѣдаешь ранъ,
Незримый хранитель могучему данъ.
Пушкинъ.

Но если въ ней единое пятно,
Единое случайно завелося,
Тогда бѣда...
Пушкинъ, „Борисъ Годуновъ“.

Мы разсмотрѣли всѣ извѣстныя намъ системы, употребляемыя у насъ революціонерами, прихватили даже нѣкоторыя такія, объ употребленіи которыхъ въ Россіи мы не имѣемъ свѣдѣній, и въ результатѣ ни одна насъ не удовлетворила. Позади насъ поле, усѣянное костями шифровъ, за которымъ чудится болѣе обширное поле, покрытое костями ихъ жертвъ. Трудно себѣ представить, сколько людей было арестовано, сослано, сколько организацій разгромлено только на основаніи расшифрованныхъ писемъ.

Идеальный шифръ долженъ обладать двумя качествами: удобствомъ примѣненія и абсолютной недоступностью.

А) Удобство примѣненія достигается тогда, когда составленіе таблицы отнимаетъ весьма мало времени и, во вторыхъ, когда пользованіе ею, т. е. выбираніе знаковъ нехлопотливо и производится быстро. Если отсутствуетъ первое условіе, т. е. если требуется слишкомъ много времени на предварительныя манипуляціи, то корреспондентъ избѣгаетъ шифровки, оставляетъ нерѣдко важныя записи незашифрованными. Получивъ письмо, гдѣ имѣется всего нѣсколько зашифрованныхъ фразъ, онъ лѣнится приступить къ разбору и письмо надолго у него залеживается: ради какихъ-нибудь 2-3 строкъ составить сложную таблицу! Лучше ужъ обождать, когда получится еще письмо или придется отвѣчать. Намъ извѣстны многіе случаи, когда при-

готовленныя таблицы сохранялись въ теченіе нѣсколькихъ дней; не сегодня-завтра придется отвѣчать на письмо и тогда опять составляй таблицу! Все это почти неизбѣжныя слѣдствія отсутствія перваго изъ условій. Если же выборка знаковъ, т. е. примѣненіе таблицы, слишкомъ затруднительна, то корреспондентъ избѣгаетъ много шифровать и наровитъ ограничиваться отдѣльными фразами или, что еще хуже, отдѣльными словами въ предложеніяхъ, вообще допускаетъ разныя непозволительныя вольности, описанныя въ предыдущей главѣ.

Б) Абсолютная надежность шифра, при условіи правильнаго зашифровыванія, достигается тогда, когда система обладаетъ *всѣми* перечисленными ниже качествами:

1) Достаточное количество знаковъ;

2) Цѣлесообразная, т. е. соотвѣтствующая фонетическимъ законамъ пропорція знаковъ;

3) Минимальная или даже абсолютная независимость знаковъ другъ отъ друга;

4) Невозможность найти во внѣшнемъ мірѣ элементы шифра, т. е. ключъ или важнѣйшую его часть;

5) Возможность контроля надъ равномѣрной утилизаціей всѣхъ знаковъ. Мы видѣли, напр., что при стихотворномъ ключѣ контроль (посредствомъ отчеркиванія) очень легокъ и полезенъ; при квадратномъ онъ крайне затруднителенъ; но тамъ дѣло обстоитъ такъ плохо, что чѣмъ больше стараться въ данномъ направленіи, тѣмъ легче разгадка; отъ безсознательнаго же отношенія тоже добра выйти не можетъ.

Читатель, можетъ быть, удивится, что мы не отмѣчаемъ здѣсь въ числѣ необходимыхъ условій *нераспознаваемость системы*, между тѣмъ какъ, напр., въ цитированномъ уже пару разъ предупрежденіи „Искры" — на это обращалось преимущественное вниманіе ея читателей. Дѣло въ томъ, что въ громадномъ большинствѣ случаевъ почти невозможно скрыть систему. Мы видѣли во всѣхъ случаяхъ разбора употребляющихся шифровъ, что „распознаваніе системы" производилось безошибочно, иногда съ перваго же взгляда, иногда — послѣ составленія подсчетной таблицы и лишь рѣдко — послѣ неудачи анализа въ одномъ направленіи; напр., *иногда* нельзя отличить стихотворнаго шифра отъ книжнаго, вторичнаго слитнаго отъ сложнаго квадратнаго. Выѣзжать, главнымъ образомъ, на незнакомой системѣ — дѣло очень рискованное; тѣ ухищренія, усложненія и фокусы, которые придумываетъ революціонеръ, ему самому кажутся и удачными, и никому неизвѣстными, въ дѣйствительности же невѣроятно, чтобы о нихъ не знало спеціальное бюро, много десятковъ лѣтъ занимающееся этими вопросами и накопившее громадный опытъ. А разъ главный рессурсъ — неизвѣстная система разгадана, то революціонеръ оказывается въ положеніи того полководца, который всѣ свои надежды возлагалъ не на хорошую армію, а на хитрый планъ военныхъ дѣйствій, и вдругъ съ ужасомъ узнаетъ, что онъ выкраденъ или разгаданъ врагами. Конечно, всякое ухищреніе, если оно не идетъ въ ущербъ прочимъ полезнымъ качествамъ шифра, — лишній плюсъ, но нельзя ставить его во главу угла и нераспознаваемость системы считать въ числѣ необходимыхъ условій хорошаго шифра. Въ силу этихъ-то соображеній мы и сочли возможнымъ изложить въ слѣдующей главѣ особую систему, которую мы считаемъ вполнѣ раціональной. Вполнѣ безупречный шифръ не долженъ бояться того, что его система извѣстна; если же онъ боится, значитъ онъ негоденъ.

Два основныхъ условія: удобство примѣненія и абсолютная надежность почти всегда стоятъ въ противорѣчіи другъ къ другу, что вполнѣ понятно: все то, что можетъ затруднять разгадку, какъ умноженіе распредѣлителей въ квадратныхъ, удлиненіе періодовъ въ гамбеттовскихъ, комбинированіе нѣсколькихъ системъ — все это дѣлаетъ примѣненіе болѣе хлопотливымъ.

Всѣмъ поставленнымъ условіямъ не удовлетворяетъ ни одна изъ разобранныхъ системъ, но все же валить ихъ въ одну кучу нельзя.

А. *Безусловно не годятся* и должны быть выброшены за бортъ: единозначные, простой квадратный, прерывистый квадратный (съ фиктивными цифрами) и почти всѣ періодическіе.

Б. *Для всякой величины* текстовъ допустимы:

а) *Книга* для небольшой опредѣленной категоріи *корреспондентовъ* (см. гл. XV).

б) *Стихотворенія* — крайне рѣдкія и неизвѣстныя — стало быть, лишь въ небольшомъ тѣсномъ кругу (см. гл. XVI).

В. *Для небольшихъ текстовъ* въ 100—300 буквъ допустимы (при правильной шифровкѣ):

а) Сложный квадратный съ нѣсколькими распредѣлителями (глава XVII—5, 6);

б) Вторичный слитный періодическій съ длиннымъ періодомъ (гл. XIV);

в) Сокращенный гамбеттовскій (гл. IX)—съ тѣмъ непремѣннымъ условіемъ, чтобы ключомъ служилъ цѣлый отрывокъ: какая-нибудь выхваченная часть стихотворенія или книги. Начать его нужно съ условленнаго пункта, гдѣ-нибудь изъ середины строки или стиха; при этомъ не будетъ надобности возвращаться опять къ началу ключа, развѣ только если мы дойдемъ до конца стихотворенія. Система перестаетъ быть періодической; это просто наложеніе одного текста на другой. Она абсолютно неразрѣшима. Если ключъ представляетъ собой часть печатнаго текста книги съ какой-нибудь условной буквы *), то въ случаѣ даже нахожденія этой книги у корреспондента и разгадки ея предназначенія, раскрытіе криптограммы отнимаетъ колоссальное количество времени. Въ книгѣ изъ 20 листовъ, т. е. 600 тысячъ буквъ, очевидно, возможно 600.000 періодовъ; чтобы ихъ перепробовать, нужно потратить, по крайней мѣрѣ, 4—6 лѣтъ! Если же еще ввести нѣкоторыя ухищренія, напр., пропускъ извѣстныхъ словъ и т. п., то рѣшеніе откладывается на такой долгій срокъ, что шифръ фактически становится вполнѣ безопаснымъ.

Шифровка отнимаетъ не очень много времени, и вообще систему можно счесть вполнѣ годной. Неудобство лишь въ томъ, что безъ книги оказывается совершенно безпомощнымъ. Еще одно неудобство, которое, на первый взглядъ, способно вызвать улыбку, но которое въ дѣйствительности можетъ оказаться предательскимъ. Благодаря частой эксплуатаціи условной страницы, она пріобрѣтаетъ потертый видъ, обычный для часто читаемаго листка, и тѣмъ рѣзко выдѣляется изъ массы остальныхъ свѣжихъ страницъ. Подобнаго рода жалобы намъ приходилось слышать и отъ лицъ, пользовавшихся одной условной страницей „книжнаго" шифра, описаннаго въ XV главѣ. Выходъ изъ обоихъ этихъ неудобствъ заключается въ томъ, чтобы заучить наизусть длинный отрывокъ изъ книги; такъ какъ распредѣленіе строкъ здѣсь не имѣетъ никакого значенія, то дѣло не представляетъ особенныхъ трудностей.

Въ случаѣ употребленія квадратныхъ системъ оказывается полезнымъ, вмѣсто однихъ только цифровыхъ знаковъ, пользоваться буквенно-цифровымъ изображеніемъ ихъ: 2а, 3б. 1щ (или просто щ), 9л и т. д. Это даетъ 34×10, т. е. 340 комбинацій. Вертикальная нумерація 1, 2, 3... 9, 0 можетъ быть замѣнена азбукой, представленной извѣстнымъ условнымъ образомъ въ 3—4 столбца. Ее можно примѣнить съ удобствомъ къ квадратнымъ системамъ.

Чтобы заключить эту главу, остановимся еще на томъ, какая азбука выгоднѣе: полная или тюремная. Для періодическихъ системъ безусловно удобнѣе вторая, но этого нельзя сказать объ ней въ приложеніи къ квадратнымъ. Главный недостатокъ послѣднихъ—плохую пропорцію буквъ—она не только не ослабляетъ, а еще усиливаетъ. Въ самомъ дѣлѣ, тюремная азбука выбрасываетъ *ѣ*, *э*, налагая ихъ функцію на *е*, которая и безъ того слишкомъ часто треплется: точно также *и* должно служить вмѣсто *і*, *й*. Поэтому нѣтъ смысла выбрасывать эти буквы, а лучше, чтобы они служили другъ за друга: е=ѣ=э (ср. слѣдующую главу).

---

*) Отрывокъ долженъ начинаться обязательно съ середины какого-нибудь слова, а не съ начала его.

Глава XX.

РАЦІОНАЛЬНЫЙ ШИФРЪ.

Онъ не измѣнитъ, онъ не обманетъ!
Лермонтовъ, „Герой нашего времени".

Моря житейскаго шумныя волны
Мы протекли.
Пристань надежную утлые челны
Здѣсь обрѣли!

Предлагаемая система, которая удовлетворяетъ всѣмъ требованіямъ, выведеннымъ нами для хорошаго, т. е. надежнаго и удобнаго шифра, принадлежитъ по внѣшнему своему виду къ категоріи квадратныхъ. Читатель не долженъ пугаться дальнѣйшихъ подробностей и кажущихся весьма сложными, на первый взглядъ, условностей. Сложность заключается только въ *изложеніи* способа, а не въ его *примѣненіи*. Для большей ясности мы разсмотримъ въ отдѣльности и по порядку его элементы:

1. Форма:
2. Содержимое (пропорція буквъ);
3. Ходъ буквенной цѣпи;
4. Порядокъ разнесенія буквъ на таблицѣ;
5. Ключъ:
   а) формула;
   б) распредѣлитель;
6. Способъ контроля;
7. Поправки:
8. Усложненія.

1) *Форма*. Мы выбрали обыкновенный квадратъ въ 10×10 клѣтокъ. Увеличивъ размѣръ, мы получили бы, конечно, болѣе широкіе предѣлы, но зато составленіе таблицы требовало бы больше времени и управляться съ ней и производить контроль было бы труднѣе. Сотни знаковъ при надлежащей пропорціи совершенно достаточно.

2) *Содержимое*. Въ пропорціи и заключается все дѣло. Имѣющаяся въ нашемъ распоряженіи сотня знаковъ распредѣлена приблизительно *пропорціонально частотѣ буквъ* въ живой рѣчи. Мы беремъ:

I	—	*12*	знаковъ для буквы	*о*	. . . . .	= 12
II	по	*7*	„ „ „	а, е, и, н, т	. . .	= 35
III	„	*5*	„ „ „	л, с	. . . .	= 10
IV	„	*4*	„ „ „	в, р	. . . .	= 8
V	„	*3*	„ „ „	д, к, м	. . . .	= 9
VI	„	*2*	„ „ „	б, г, п, у, ы, я	. . . .	= 12
VII	„	*1*	„ „ „	ж, з, і, й, ф, х, ц, ч, ш, щ, ь, ѣ, э, ю	. . .	= 14
Итого: 7 категорій,				33 буквы,		100 знаковъ.

Изъ всего алфавита выброшена только буква ъ, какъ совершенно безполезная. Прочія сохранены, такъ какъ даже самыя рѣдкія могутъ оказаться необходимыми и незамѣнимыми въ адресахъ, фамиліяхъ и т. п.

Приведенныя отношенія обязательно нужно запомнить. Сдѣлать это очень легко, если прибѣгнуть къ нѣкоторымъ мнемоническимъ пріемамъ. Можно, напр., изъ буквъ каждой категоріи составить слово: изъ а, е, и, н, т — Антей; изъ д, к, м, — домик и т. д. (вставочныя соединительныя буквы, какъ въ послѣднемъ примѣрѣ — о, и, — не будутъ мѣшать и путать, если онѣ уже имѣются въ высшихъ категоріяхъ).

Четырнадцать разовыхъ буквъ послѣдней категоріи тоже легко запомнить, если обратить вниманіе на то, что четыре изъ нихъ: ж, з, і, й, идутъ подрядъ въ концѣ перваго отдѣла азбуки (см. табл. № 5), а остальныя десять: ф, х, ц, ч, ш, щ, ъ, ѣ, э, ю — составляютъ III отдѣлъ — рѣдкихъ буквъ, почти сплошную часть алфавита (не хватаетъ только ъ, совсѣмъ отсутствующаго, и *ы*, *я*, причисленныхъ къ предшествующей категоріи).

Наконецъ, чтобы еще болѣе облегчить запоминаніе представленныхъ отношеній (вѣдь это гвоздь системы), мы изобразили ихъ въ формѣ виршей, построенныхъ по образцу знаменитыхъ

„Много есть именъ на is"...

Правда, классикъ придетъ въ ужасъ отъ того, во что мы превратили игривый мифъ про царскую дочь Іо, превращенную ревнивой Юноной въ корову и преслѣдуемую шершнемъ; но если вѣрить „профессору мнемоники" Файнштейну, то чѣмъ нелѣпѣе мнемоническая формула, тѣмъ легче ее запомнить. Вотъ эти вирши:

Двѣнадцать лѣтъ блуждала *о*, но къ ней
Былъ посланъ на *седьмомъ* году *Антей*.
Пять лѣтъ гонялъ ее со всѣхъ онъ *сил*,
Пока на *четырехъ* свалилась въ *ров*,
Что съ *трехъ* сторонъ нашъ *домик* окружилъ.
Когда-бъ я это зналъ, то *я бы плуг*
Вкругъ хижины съ боковъ обвелъ лишь съ *двухъ*.
И сталъ я звать по *одному* рабовъ:
Же-зе, і съ точкой, й съ крючкомъ, ко рв!
Эф-ха; це-че; ша-ща; ерь-ять; э-ю!

3) *Ходъ буквенной цѣпи.* Положимъ, что мы заучили предыдущее стихотвореніе, и пропорція буквъ крѣпко засѣла въ нашей памяти. Какъ же, спрашивается, нанести ихъ на таблицу? Очевидно, что всѣ обычные способы квадратныхъ шифровъ здѣсь непримѣнимы. Прежде всего нужно составить изъ нашихъ 100 буквъ одну непрерывную цѣпь. Способъ, который мы называемъ *нормальнымъ*, заключается въ томъ, что буквы нанизываются именно въ томъ порядкѣ, въ какомъ онѣ приведены въ мнемоническомъ стихотвореніи. Сперва пишемъ двѣнадцать *о*, потомъ семь *а*, семь *н*, семь *т* и т. д.: 12о+7а+7н+7т+7е+7и+5с+5л+4р+4в+3д+3м+3к+2я+2б+2ы+ +2п+2у+2г+ж+з+і+й+ф+х+ц+ч+ш+щ+ь+ѣ+э+ю.

Это будетъ *нормальная* цѣпь. Можно, конечно, составить другую цѣпь, т. е. держаться другого расположенія. Напр., можно писать ее въ обратномъ порядкѣ: начать съ *ю* и кончить двѣнадцатью *о*. Можно также въ каждомъ мнемоническомъ словѣ (т. е. въ каждой категоріи) писать буквы въ другомъ порядкѣ, напр. во II-ой категоріи — „Антей" писать 7и+7е+7т+7н+7а и т. д. Можно еще писать раньше тѣ буквы, которыя повторяются четное число разъ (12о+4р+4в+2я и т. д)., а потомъ тѣ, которыя берутся нечетное число разъ. Вообще можно придумать много комбинацій для составленія буквенной цѣпи, но *если способа не указано заранѣе, то обязательно предполагается нормальный порядокъ.*

4) *Порядокъ разнесенія цѣпи.* Прежде всего нуженъ исходный пунктъ, т. е. опредѣленная, заранѣе условленная клѣтка изъ ста клѣтокъ таблицы. Она обозначается *формулой*, о которой рѣчь ниже. Начиная съ исходной клѣтки, буквы наносятъ, придерживаясь слѣдующихъ правилъ:

а) Буквы идутъ обязательно по діагоналямъ, подобно „слонамъ" въ шахматной игрѣ;

б) Неизмѣнно по направленію часовой стрѣлки. Это значитъ, что книзу отъ главныхъ діагоналей онѣ идутъ справа налѣво, а сверху отъ нихъ — слѣва направо. Въ самихъ же діагональныхъ полосахъ направленіе ихъ зависитъ отъ того, съ какой стороны онѣ въ нихъ вступили, и обязательно совпадаетъ съ движеніемъ часовой стрѣлки;

в) Всякій разъ, когда буквенная цѣпь подходитъ къ *лѣвому* краю, она подымается на одну клѣтку вверхъ (подобно ладьѣ въ шахматной игрѣ); если сосѣдняя клѣтка уже занята, то она ползетъ по направленію часовой стрѣлки по краю до первой свободной клѣтки, хотя бы таковая нашлась только на верхней сторонѣ, а то даже на правой — или нижней; послѣ этого она снова идетъ по діагонали.

Ниже помѣщенъ цѣлый рядъ образчиковъ для упражненія (табл. №№ 58—64).

Таблица № 58. Формула $^{8}/_{9}$.

	1	2	3	4	5	6	7	8	9	0
1	44	29	12	58	70	80	88	94	98	100
2	28	11	30	13	59	71	81	89	95	99
3	10	43	45	31	14	60	72	82	90	96
4	9	27	42	46	32	15	61	73	83	91
5	57	8	26	41	47	33	16	62	74	84
6	69	56	7	25	40	48	34	17	63	75
7	79	68	55	6	24	39	49	35	18	64
8	87	78	67	54	5	23	38	50	1	19
9	93	86	77	66	53	4	22	2	20	36
0	97	92	85	76	65	52	3	21	37	51

Таблица № 59. Формула $^{4}/_{3}$.

	1	2	3	4	5	6	7	8	9	0
1	4	20	37	52	65	76	85	92	97	100
2	3	5	21	38	53	66	77	86	93	98
3	36	2	6	22	39	54	67	78	87	94
4	51	35	1	7	23	40	55	68	79	88
5	64	50	34	19	8	24	41	56	69	80
6	75	63	49	33	18	9	25	42	57	70
7	84	74	62	48	32	17	10	26	43	58
8	91	83	73	61	47	31	16	11	27	44
9	96	90	82	72	60	46	30	15	12	28
0	99	95	89	81	71	59	45	29	14	13

Таблица № 60. Формула $^{3}/_{0}$.

	1	2	3	4	5	6	7	8	9	0
1	89	82	73	62	49	34	17	95	98	100
2	81	72	61	48	33	16	35	18	96	99
3	71	60	47	32	15	63	50	63	19	1
4	59	46	31	14	83	74	64	51	2	20
5	45	30	13	88	90	84	75	3	21	37
6	29	12	70	80	87	91	4	22	38	52
7	11	44	58	69	79	5	23	39	53	65
8	10	28	43	57	6	24	40	54	66	76
9	94	9	27	7	25	41	55	67	77	85
0	97	93	8	26	42	56	68	78	86	92

Таблица № 61. Формула $^{1}/_{0}$.

	1	2	3	4	5	6	7	8	9	0
1	99	96	91	84	75	64	51	36	19	1
2	95	90	83	74	63	50	35	18	2	20
3	89	82	73	62	49	34	17	3	21	37
4	81	72	61	48	33	16	4	22	38	52
5	71	60	47	32	15	5	23	39	53	65
6	59	46	31	14	6	24	40	54	66	76
7	45	30	13	7	25	41	55	67	77	85
8	29	12	8	26	42	56	68	78	86	92
9	11	9	27	43	57	69	79	87	93	97
0	10	28	44	58	70	80	88	94	98	100

Таблица № 62. Формула $^{1}/_{1}$.

	1	2	3	4	5	6	7	8	9	0
1	1	2	20	37	51	64	74	83	89	94
2	19	100	3	21	38	52	65	75	84	90
3	36	18	99	4	22	39	53	66	76	85
4	50	35	17	98	5	23	40	54	67	77
5	63	49	34	16	97	6	24	41	55	68
6	73	62	48	33	15	91	7	25	42	56
7	82	72	61	47	32	14	78	8	26	43
8	88	81	71	60	46	31	13	57	9	27
9	93	87	80	70	59	45	30	12	28	10
0	95	92	86	79	69	58	44	29	11	96

Таблица № 63. Формула $^{0}/_{0}$.

	1	2	3	4	5	6	7	8	9	0
1	10	11	29	45	59	71	81	89	95	99
2	28	9	12	30	46	60	72	82	90	96
3	44	27	8	13	31	47	61	73	83	91
4	58	43	26	7	14	32	48	62	74	84
5	70	57	42	25	6	15	33	49	63	75
6	80	69	56	41	24	5	16	34	50	64
7	88	79	68	55	40	23	4	17	35	51
8	94	87	78	67	54	39	22	3	18	36
9	98	93	86	77	66	53	38	21	2	19
0	100	97	92	85	76	65	52	37	20	1

На этихъ таблицахъ буквы замѣнены числами — послѣдовательной нумераціей — для болѣе нагляднаго изображенія хода цѣпи. Таблицы разнятся между собой, исключительно благодаря различію исходныхъ пунктовъ, т. е. „формулъ". Послѣдняя обозначается дробью, гдѣ числитель указываетъ номеръ горизонтальнаго ряда, а знаменатель — вертикальнаго столбца.

Если нѣсколько поупражняться, то записываніе цѣпи при любой формулѣ производится быстро и безошибочно.

Разумѣется, если двигаясь по діагонали, цѣпь натыкается на занятыя уже раньше клѣтки, то она черезъ нихъ перескакиваетъ.

Можно условиться и относительно другой системы нанесенія цѣпи, напр., въ направленіи, обратномъ движенію часовой стрѣлки, но если этого не сдѣлано, то обязательно предполагается вышеописанный способъ, который мы называемъ *нормальнымъ*.

Таблица № 64. Формула $^{0}/_{1}$.

	1	2	3	4	5	6	7	8	9	0
1	98	93	88	79	70	57	44	27	10	99
2	92	87	78	69	56	43	26	9	28	11
3	86	77	68	55	42	25	8	58	12	29
4	76	67	54	41	24	7	80	13	30	45
5	66	53	40	23	6	94	14	31	46	59
6	52	39	22	5	97	15	32	47	60	71
7	38	21	4	85	16	33	48	61	72	81
8	20	3	65	17	34	49	62	73	82	89
9	2	37	18	35	50	63	74	83	90	95
0	*1*	19	36	51	64	75	84	91	96	100

5) *Ключъ.* Онъ состоитъ изъ двухъ или вѣрнѣе трехъ элементовъ: вышеупомянутой „формулы" и двухъ „распредѣлителей": горизонтальнаго и вертикальнаго. Они всѣ вмѣстѣ могутъ заключаться въ любой условной фразѣ или стихѣ, вслѣдствіе чего достаточно только условиться о таковой, чтобы этимъ опредѣлились и формула и распредѣлители.

Пусть, напр., ключомъ служитъ стихъ: *Когда же слезами до самаго края...* Отдѣляемъ въ немъ слѣва сперва *десять* буквъ, потомъ еще *десять* и наконецъ *двѣ*. Первые два десятка дадутъ намъ распредѣлителей, послѣднія двѣ буквы „*го*" — „формулу". Понумеровавши въ распредѣлителяхъ буквы сообразно мѣсту ихъ въ алфавитѣ, получаемъ слѣдующія числа (ср. гл. V и XVII, 5):

1) к о г д а ж е с л е | з а м и д о с а м а | г о | к р а я
7 9 2 3 1 6 4 0 8 5 | 5 1 7 6 4 9 0 2 8 3 | | |

Для полученія числового выраженія формулы „*го*" поступаемъ такъ: первую букву *г* ищемъ въ первомъ распредѣлителѣ, находимъ таковую и подъ ней цифру 2; это будетъ числителемъ: вторую букву *о* ищемъ во второмъ распредѣлителѣ, гдѣ подъ таковой стоитъ цифра 9; это будетъ знаменателемъ. Слѣдовательно формула — $^{2}/_{9}$ или 29. Если бы тождественныхъ буквъ не оказалось, то слѣдовало бы взять ближайшія меньшія (по алфавиту). Вотъ еще примѣры:

2) Н а с т у п и л и о | т в р а т и т е л ь | н ы | я п о г о д ы
5 1 8 9 0 7 2 4 3 6 | 7 2 6 1 8 4 9 3 5 0 | *5 7* |

Здѣсь первая буква формулы *н* имѣется въ первомъ распредѣлителѣ, вторая же *ы* не находится; ближайшей буквой къ ней является *т*, а такъ какъ ихъ тамъ имѣется цѣлыхъ три экземпляра, то мы беремъ первый съ цифрой 7. Формула поэтому 57.

3) Т о г д а с м и р я | е т с я д у ш и м о | е й | т р е в о г а
9 6 2 3 1 8 5 4 7 0 | 2 7 6 0 1 8 9 3 4 5 | *3 3* |

4) Н е с е т с я к о ф | р а н ц і и м и л о | й г | д ѣ...
4 1 6 2 8 7 0 3 5 9 | 9 1 7 0 4 2 6 3 5 8 | *1 1* |

Это будетъ *нормальный* способъ полученія „формулы". Можно придумать и иные, напр. просто условиться относительно какого-нибудь двузначнаго числа, совершенно независимо отъ фразы. Но если не указаны другіе способы, то необходимо предполагать нормальный.

По формулѣ отыскиваемъ исходную клѣтку (числитель=горизонтальному ряду,

знаменатель=вертикальному), разносимъ буквы, надписываемъ распредѣлителей, первый вверху, второй по лѣвому краю—и таблица готова. (См. табл. № 65).

6) *Контроль.* Способъ записыванія буквъ не представляетъ ничего особеннаго. Каждая буква отмѣчается двумя цифрами, изъ коихъ одна обозначаетъ горизонтальный рядъ, а другая—вертикальный. Напр., фраза „намъ нуженъ наборщикъ" можетъ быть выражена по таблицѣ № 65 (ключъ „когда же слезами до самаго края..."): „789903815938116504632575675009 19". Благодаря цѣлесообразной пропорціи буквъ, знаки будутъ утилизироваться равномѣрно, но лишь въ томъ случаѣ, если шифрующій будетъ относиться къ дѣлу сознательно, если онъ будетъ стараться использовать *всѣ* знаки каждой буквы, а не хвататься за первыя попавшіяся. Контроль здѣсь вести весьма легко. Въ стихотворномъ ключѣ мы достигаемъ этого отчеркиваніемъ использованныхъ буквъ. Здѣсь же нужно отмѣчать черточкою каждую утилизированную клѣтку. Число черточекъ будетъ расти довольно равномѣрно, и незатронутыя клѣтки сейчасъ же будутъ бросаться въ глаза. Чтобы выполнить это чище и толковѣе, надо съ самаго начала сдѣлать квадратъ правильнымъ, аккуратно разлиненнымъ (лучше всего пользоваться готовой бумагой—въ клѣточкахъ), буквы вписывать ближе къ верхнему краю клѣтокъ, а черточки ставить на нижней окраинѣ; при текстѣ изъ 300 буквъ на каждую клѣтку придется три черточки (см. таблицу № 66, гдѣ нанесены образцы черточекъ отъ 1 до 12). Нѣтъ надобности брать всѣ экземпляры одной буквы, напр. всѣ 12 *о подрядъ*, а лучше брать ихъ въ разбивку, какая изъ нихъ попадется на глаза. Также нѣтъ надобности тогда только взять вторично какой-нибудь изъ знаковъ *о*, когда у насъ уже перебывали всѣ 12. Не бѣда, и даже гораздо лучше, если нѣкоторые изъ нихъ пойдутъ уже второй разъ, въ то время когда иные еще не были въ дѣлѣ. Послѣ это уравняется, но совершеннаго уравненія и нежелательно. Положимъ, напр., что въ текстѣ имѣется всего 48 экземпляровъ буквы *о*. На каждую клѣтку таблицы придется такимъ образомъ, въ среднемъ, 4 экземпляра. Не бѣда, если нѣкоторые будутъ утилизированы и 5 разъ и 6 разъ, а другіе—всего 3 раза.

Таблица № 65. Формула 29.

	7	9	2	3	1	6	4	0	8	5
5	й	у	к	в	с	е	а	щ	ь	ю
1	и	к	в	с	е	а	е	а	*о*	ѣ
7	к	р	с	т	а	в	с	е	н	о
6	р	и	т	а	у	я	в	с	о	н
4	н	т	а	і	ф	г	я	о	н	е
9	т	а	м	п	з	х	о	н	е	л
0	о	и	р	м	ы	о	н	е	л	д
2	о	т	п	р	о	н	и	л	д	б
8	ш	о	т	о	н	и	л	д	б	г
3	э	ч	о	т	и	л	м	ы	ж	ц

Таблица № 66.

1	2	3
I	II	III
4	5	6
IIII	IIIV	IIIVI
7	8	9
IIIVII	IIIVIII	IIIVIIII
10	11	12
IIIVIIIX	IIIVIIIXI	IIIVIIIXII

7) *Поправки.* Цѣль системы заключается въ томъ, чтобы всѣ знаки утилизировались вполнѣ одинаково. Однако, на практикѣ такой идеалъ невозможенъ. Если бы пропорціи были даже вполнѣ безукоризненны, т. е. въ точности соотвѣтствовали фонетическимъ законамъ, то все же мы никогда бы не достигли одинаковыхъ коэффиціентовъ для всѣхъ клѣтокъ, ибо въ каждомъ отрывкѣ, хотя бы онъ и заключалъ нѣсколько тысячъ буквъ, пропорція ихъ сильно отступаетъ отъ выведенныхъ нами въ I-ой главѣ среднихъ, и чѣмъ текстъ меньше, тѣмъ больше колебанія. Но помимо того, пропорціи буквъ, которыя мы ввели въ разбираемой системѣ, не могутъ быть совершенными: буква *о*, напр., разъ въ тысячу употребительнѣе *ф*. На пространствѣ 100 буквъ нашей таблицы такихъ отношеній ввести невозможно, и у насъ *о* лишь въ 12 разъ больше представлена, чѣмъ *ф*. Можно было бы, конечно, вовсе выбросить рѣдкія буквы, но мы предпочли ихъ сохранить для тѣхъ случаевъ, когда онѣ могутъ оказаться необходимыми. Зато тутъ оказывается необходимость ввести извѣстные коррективы, поправки.

Они заключаются въ томъ, что родственныя буквы замѣняютъ другъ друга, и

въ случаѣ чрезмѣрной частоты въ текстѣ одной буквы, она питается насчетъ близкихъ по созвучію. 1) э=ѣ. Клѣткой э надо пользоваться для замѣщенія *ѣ*, какъ еслибы въ ней была изображена эта послѣдняя буква. Но, кромѣ того, обѣ онѣ могутъ сходить и за *е* и обратно. 2) ф=п=в. Какъ выше мы взяли для *ѣ* коэффиціентъ 1 вмѣсто 2, имѣя въ виду уравновѣсить ее посредствомъ рѣдкой э, такъ и здѣсь мы имѣемъ для *п* — 2 вмѣсто 3, потому что эта буква должна быть уравновѣшена посредствомъ *ф*. 3) ш=щ=сч=с. 4) і=й=и=ы. 5) ж=з=г. 6) ю=у=іу. 7) я=а=іа. 8) ц=ч. 9) м=н. 10) к=х.

Разумѣется, въ изображеніи адресовъ, фамилій и т. п. замѣна буквъ не допускается, но во всѣхъ другихъ случаяхъ она нисколько не препятствуетъ пониманію словъ, тѣмъ болѣе, что знаешь, какія буквы замѣняютъ другъ друга. Напишемъ ли мы „полючилъ“ или „полуцилъ“, или „поліучил“ — все равно, сейчасъ же будетъ понято, что это значитъ „получилъ“. Впрочемъ, больше одной замѣны въ словѣ дѣлать не слѣдуетъ.

Полезно иногда тѣ буквы, которыя упорно не попадаются въ текстѣ, помѣщать безъ всякой надобности въ концѣ какого нибудь слова, напримѣръ, „Вышлитец по такому...“

8) *Усложненія.* Система допускаетъ различныя усложненія, которыя отнимаютъ весьма мало времени. Напр., можно ввести 1 или 2 лишнихъ распредѣлителя, для чего нужно только продолжить нашъ стихъ еще на двадцать буквъ. Если это продѣлать съ тѣмъ стихомъ, который послужилъ ключомъ для табл. № 65, то получимъ такіе два новыхъ распредѣлителя:

Когда же сле	зами до сама	го	к р а я н а п о л н	и т с я ч а ш а с в	я т а я
			3 9 1 0 5 2 8 7 4 6	4 7 5 0 8 1 9 2 6 3	

Ихъ надо написать на той же таблицѣ, лучше всего, во избѣжаніе путаницы, одинъ (первый) — *внизу*, другой — *справа* (ср. табл. № 68), и затѣмъ пользоваться попеременно то одними, то другими, по образцу множественнаго квадратнаго шифра (гл. VII), или описаннаго въ гл. XVII, 6; знакомъ перехода должна служить либо *пара* одинаковыхъ буквъ, либо что-нибудь другое; можно и безъ сигналовъ. Отмѣчать черточками *клѣтки* съ цѣлью равномѣрной ихъ утилизиціи нужно и здѣсь, хотя въ данномъ случаѣ равномѣрности *знаковъ* уже не будетъ.

Можно ввести и другія осложненія, напримѣръ., замѣну въ вертикальномъ распредѣлителѣ цифръ буквами азбуки, подобно тому, какъ это изложено въ предыдущей (XIX) главѣ. Но, въ сущности говоря, эти осложненія совершенно излишни.

Задача. 3381826368102949589706134142090265405715664783969824037926270412333743056754725621557138979201298527309134228683787331802228446108361062866505826495930490518462767546062599145391887715130778161988894437502435016657455070117230093422188279745440787468314289439400080923487045721002906720173871129169604795368593274111394381386569489989507662641652239419073960285453570216528600259884131806449626831287862978038433794208590964480787930135553127673274309052053988725560768382157158541162646077683265579932662324224759077463517526493450482941983546552779436542258192281993530008802058958821560907953117914589164069906818950315857614968066583856062473919961467402200139214650712372224760928461826381836496527394671411104137940907192939832848923700440440210399371379748063867053253462055758514315908110675153046944261749076328368459600266115447621710239155147559704543123631565422695031299686510550554998383301857759418865207900133524560932897598067134227508811076721251803506839629787391644044285066685614306516553917572625021815437630208593334290452085012715574037139916936208868333477461782682113372978746.

Распознаваніе системы. Здѣсь 551 пара цифръ. Составимъ подсчетную таблицу (таб. № 67). Достаточно лишь кинуть на нее взглядъ, чтобы угадать систему. Такого равномѣрнаго распредѣленія знаковъ не даетъ ни одинъ шифръ.

Раскрытіе шифра. Совсѣмъ иное однако дѣло, когда, распознавши систему, мы попытаемся пойти дальше. Та же равномѣрность частоты знаковъ, которая выдаетъ ее головой, дѣлаетъ безплоднымъ всякій анализъ. Благодаря ей нельзя узнать, гдѣ скрываются перворазрядныя буквы, и гдѣ рѣдкія. Раньше, при обзорѣ другихъ системъ, мы видѣли, что чѣмъ больше текстъ, тѣмъ болѣе увеличиваются шансы разгадки. Здѣсь же этого совершенно нѣтъ: наоборотъ, чѣмъ длиннѣе текстъ, тѣмъ ближе подходятъ пропорціи системы къ фонетическимъ, и слѣдовательно, тѣмъ

равномѣрнѣе становится частота буквъ. Зато чѣмъ меньше текстъ, тѣмъ она можетъ быть слабѣе выражена, благодаря сильнымъ уклоненіямъ текста отъ фонетическихъ пропорцій. Не является ли это гибельнымъ? Нисколько. Отклоненія, которыя бываютъ въ небольшихъ текстахъ, до такой степени разнообразны, что никоимъ образомъ невозможно узнать, какія буквы здѣсь преобладаютъ. Самымъ частымъ зна омъ можетъ оказаться какое нибудь *ш* или *і*, а рѣдкимъ — *о*. Такимъ образомъ ни въ большихъ текстахъ, ни въ малыхъ нельзя найти никакого исходнаго пункта, никакой руководящей нити для разгадки.

Таблица № 67.

	1	2	3	4	5	6	7	8	9	0
1	6	5	6	5	7	6	5	4	4	7
2	4	7	5	5	5	5	6	6	7	6
3	6	4	7	5	5	4	6	5	6	5
4	5	6	6	6	5	5	6	5	4	6
5	5	4	5	6	8	6	7	5	5	8
6	4	7	5	6	7	6	5	5	5	6
7	5	7	4	7	5	6	3	6	6	4
8	6	6	8	5	6	6	3	5	5	6
9	7	4	6	4	5	5	3	5	6	6
0	6	6	4	4	5	6	7	6	7	5

Нельзя ли, однако, подойти къ дѣлу съ другой стороны? Вѣдь мы знаемъ и пропорцію буквъ, и порядокъ ихъ разнесенія на таблицѣ. Самое число возможныхъ табличекъ довольно ограниченное: ихъ столько, сколько исходныхъ клѣтокъ, т. е. сто. Разнообразіе сочетаній дается, главнымъ образомъ, распредѣлителями. Нельзя ли поэтому, пользуясь небольшимъ количествомъ возможныхъ табличекъ, *подобрать* распредѣлителей? Вѣдь здѣсь дѣло обстоитъ какъ будто хуже, чѣмъ въ сложномъ квадратномъ шифрѣ, въ которомъ составъ таблицы *вовсе* неизвѣстенъ. Увы, и съ этой стороны мы встрѣчаемъ полнѣйшее фіаско. Если бы даже исходный пунктъ былъ извѣстенъ, т. е. если бы мы могли составить полную табличку въ родѣ табл. № 65, то и это ни къ чему бы не повело, такъ какъ число возможныхъ перестановокъ въ ней, производимыхъ обоими распредѣлителями, достигаетъ ни болѣе, ни менѣе, какъ 13168189440000! При неизвѣстности же и „формулы", т. е. исходной клѣтки, число всѣхъ возможныхъ комбинацій доходитъ до $1^1/_2$ квадрильоновъ. Чтобы перепробовать ихъ, с итая по 3 минуты на пробу и 12-часовой рабочій день, надо потратить 15321797 столѣтій. Можно, пожалуй, и согласиться на разгадку черезъ такой періодъ времени.

Найти во внѣшнемъ мірѣ элементы ключа, конечно, нѣтъ возможности. Это не книга и не стихотвореніе. Ключъ состоитъ изъ одной коротенькой фразы или вырваннаго гдѣ-нибудь стиха. Добраться до чего-нибудь посредствомъ анализа текста тоже нельзя: на разстояніи многихъ десятковъ буквъ не повторяется ни одинъ знакъ. Никакой закономѣрности въ ихъ расположеніи найти нельзя. Если бы даже было угадано какое-нибудь слово и мы получили бы такимъ образомъ значенія нѣсколькихъ знаковъ, то добраться при помощи ихъ до остальныхъ нѣтъ возможности, ибо намъ неизвѣстенъ истинный порядокъ ни вертикальныхъ, ни горизонтальныхъ рядовъ.

Таблица № 68.

	7	9	2	3	1	6	4	0	8	5	
5	Л7	И5	Я4	О5	В8	Я6	Г6	Х8	Ь5	Ю8	4
1	И5	П4	О5	Т6	О6	Д6	Б5	Г7	Ц4	Ъ7	7
7	И3	О6	Л7	И4	Т5	О6	Д7	Б4	Ж6	Ч5	5
6	О5	И5	Л7	Р5	П4	Т6	О6	Д6	Ю5	З7	0
4	А6	Н4	Е5	Л7	Р5	И5	Т6	А6	М5	Ы5	8
9	Я3	О6	Н4	Е6	Л7	Р6	П4	Т6	А5	М5	1
0	У7	К7	О6	Н4	Е6	С6	Р4	С5	Т6	А5	9
2	Ф6	У7	К7	О5	Н4	Е6	С5	В6	А6	Т5	2
8	Щ3	Й5	П6	К8	О6	А6	Е5	Ц6	Е5	С6	6
3	Г6	Ш6	І4	П7	М6	В4	А5	Е5	С5	В5	3
	3	9	1	0	5	2	8	7	4	6	

Приведенный выше текстъ представляетъ собою зашифрованную басню Крылова „Стрекоза и Муравей". Мы уже раньше знали, что въ ней нѣтъ ни одного *ф* или *щ*, всего 1 *ц* и т. д. Понятно, что пришлось прибѣгать къ замѣнѣ ихъ родственными буквами. Если расшифровать при помощи ключа (на табл. № 68 нанесенъ развернутый ключъ: „Когда же слезами до самаго края", но фомула взята не „нормальная", а $^3/_5$)*), то найдемъ такія слова, какъ „оглянются", „успѣла", „пушда", „злоі", „фропѣла", „нуравей" и т. д.

*) Нижній и правый распредѣлители не имѣютъ никакого отношенія къ данному случаю; они помѣщены только для иллюстраціи сказаннаго раньше объ „усложненіяхъ" разбираемой системы.

На таблицѣ № 69 нанесено распредѣленіе знаковъ въ первой сотнѣ текста. Насколько осуществлена однородность въ большихъ и меньшихъ отрѣзкахъ текста, показываетъ таблица № 70. Изъ нея мы видимъ, что въ то время какъ для 100 буквъ среднимъ является 1 буква на клѣтку, колебанія въ дѣйствительности, оказываются въ предѣлахъ 0—2. Для 200 буквъ — колебанія 0—3, для 400 буквъ — 2—6 и т. д.

Таблица № 69.

	1	2	3	4	5	6	7	8	9	0
1	—	1	2	1	2	1	—	—	1	2
2	1	2	—	1	1	1	2	1	2	—
3	1	—	2	1	—	1	1	1	—	1
4	1	1	1	2	—	1	1	—	1	1
5	1	—	1	1	1	1	1	1	—	—
6	1	2	1	1	2	1	1	1	—	—
7	1	1	1	—	1	1	1	2	1	—
8	1	2	2	1	1	1	—	2	1	1
9	2	1	1	—	1	1	2	1	1	1
0	1	1	1	2	2	2	2	1	1	—

Таблица № 70.

	0	1	2	3	4	5	6	7	8
100	20	60	20	—	—	—	—	—	—
200	2	19	55	24	—	—	—	—	—
300	—	3	26	42	25	4	—	—	—
400	—	—	8	17	43	28	4	—	—
500	—	—	1	5	22	44	19	8	1
551	—	—	—	3	14	33	34	13	3

Заключеніе. Надежность шифра не подлежитъ сомнѣнію. Здѣсь на лицо всѣ тѣ необходимыя условія, которыя были указаны нами въ предыдущей главѣ. Во избѣжаніе всякихъ случайностей, шифрующій долженъ только имѣть въ виду, чтобы экземпляры какой-либо буквы текста *не* распредѣлились между соотвѣтственными клѣтками таблицы вполнѣ поровну, а съ небольшой разницей, какъ мы уже выше упоминали. Остается только сказать нѣсколько словъ о примѣненіи. Пропорція буквъ, ходъ цѣпи и все остальное одни и тѣ же для всѣхъ корреспондентовъ и для всѣхъ случаевъ, хотя бы ихъ были сотни. Поэтому, если поупражняться полчаса надъ способомъ нанесенія буквъ на таблицу, то составленіе ея для всякаго отдѣльнаго случая потребуетъ не больше времени, чѣмъ составленіе обыкновенной таблички квадратнаго шифра, гораздо меньше, чѣмъ выписываніе стихотворенія. Примѣненіе раціональнаго шифра, поэтому, одно изъ наиболѣе легкихъ.

„Я не знаю, можетъ ли человѣческое остроуміе изобрѣсти такой шифръ, котораго человѣческое же остроуміе не въ силахъ было бы разгадать, взявшись за дѣло надлежащимъ образомъ“ — такъ разсуждаетъ у Поэ умный Легранъ. Намъ же думается что запутывать узелъ гораздо легче, чѣмъ распутывать, и что описанный здѣсь шифръ, если его примѣнять „надлежашимъ образомъ“, принадлежитъ къ тѣмъ, гдѣ человѣческое остроуміе окажется безсильнымъ.

Заключеніе.

НЕОБХОДИМЫЯ ПРЕДОСТОРОЖНОСТИ *).

(Адреса. Походный шифръ. Адресаты. Оказіи. Тюремная переписка и проч.).

Чтобы исчерпать по возможности свою тему, мы здѣсь коснемся нѣсколькихъ частныхъ вопросовъ, заслуживающихъ по разнымъ причинамъ особаго вниманія.

1) *Адреса.* Объ адресахъ стоитъ поговорить особо потому, что они имѣютъ слишкомъ большое значеніе для революціонной организаціи, и раскрытіе ихъ зачастую приноситъ неисчислимый вредъ. Адреса бываютъ разные: для писемъ, нелегальныхъ посылокъ, явокъ; адреса революціонеровъ, конспиративныхъ квартиръ, типографій и т. п. Легко себѣ представить, сколько бѣдъ должно принести открытіе жандармами такихъ адресовъ. Если они узнаютъ адресъ для писемъ, они обыкновенно задерживаютъ ихъ, прочитываютъ, отсылаютъ по назначенію и въ то же время устраиваютъ тщательное наблюденіе за адресатомъ. Если имъ удается заполучить адресъ для явки, они посылаютъ ловкаго провокатора, который выдаетъ себя за иногороднаго революціонера и нерѣдко вывѣдываетъ, благодаря неконспиративности и довѣрчивости своихъ собесѣдниковъ, много цѣнныхъ свѣдѣній. Разумѣется, въ результатѣ подобныхъ исторій бываютъ массовые провалы.

Несмотря на такую важность адресовъ, они, однако, больше чѣмъ что-нибудь другое имѣютъ шансы попасть въ руки жандармовъ и быть разобранными. Они могутъ достаться имъ не только въ перехваченныхъ письмахъ, какъ на конвертахъ, такъ и внутри текста, но и при обыскахъ, потому что ихъ обыкновенно, не надѣясь на свою память, сохраняютъ записанными на бумажкѣ. Людямъ, на долю которыхъ выпадаетъ вести „внѣшнія" сношенія, въ качествѣ членовъ мѣстныхъ и центральныхъ комитетовъ и проч., приходится держать записанными нерѣдко 20-30 и болѣе адресовъ. Оставляя въ сторонѣ тѣ, къ стыду нашему, еще очень многочисленные случаи, когда адреса бываютъ записаны обыкновеннѣйшимъ образомъ, безъ всякаго шифра, мы должны признать, что если они даже зашифрованы и притомъ по безупречной системѣ, то они все же, благодаря специфическимъ своимъ свойствамъ, заключаютъ въ себѣ возможность раскрытія. Всякій адресъ обыкновенно содержитъ *городъ, слово* „улица" и ея названіе, оканчивающееся большей частью на „ская", слова „домъ", „квартира", „для"; нерѣдко при этомъ въ скобкахъ или безъ нихъ бываетъ отмѣчено шифромъ: „для явки", „для посылокъ", „для заказныхъ", „до востребованія" и т. п. Возьмемъ, напр., бывшій уже у насъ раньше въ дѣлѣ адресъ и отмѣтимъ въ немъ курсивомъ избитыя слова и слоги: „Самара, Казан*ская улица*, *домъ* графа Шувалова, *квартира* третья, Эртелю *для* Саши, *въ двухъ конвертахъ*".

Имѣя передъ собой зашифрованный текстъ, и зная, что это адресъ (на найденныхъ при обыскахъ запискахъ послѣднее обстоятельство сразу опредѣляется), „бюро" также знаетъ цѣлый рядъ словъ, въ немъ заключающихся; остается только пріурочить ихъ къ опредѣленнымъ группамъ цифръ, что достигается безъ большого труда послѣ нѣсколькихъ пробъ. Оно знаетъ, напр., что гдѣ-то въ началѣ отрывка заключается слово „улица", оно пробуетъ одну группу изъ 5 буквъ; если разультатовъ не получаетъ, подвигается на одну цифру вправо и снова пробуетъ и т. д., и очень скоро, конечно, натыкается на истинное сочетаніе знаковъ. Если же въ его

*) Нѣкоторыя указанія въ „заключеніи" и „приложеніи", вѣроятно, удивятъ читателя своей крайней элементарностью. Но въ средѣ революціонеровъ замѣчается такая беззаботность относительно самыхъ простыхъ требованій конспираціи, что мы сочли себя вынужденными говорить также о вещахъ, несомнѣнно принадлежащихъ къ категоріи само собою разумѣющихся.

рукахъ не одинъ адресъ, а цѣлая коллекція ихъ, захваченная въ одномъ мѣстѣ, то дѣло чрезвычайно облегчается. Стоитъ только одному знаку повториться въ однородномъ участкѣ разныхъ адресовъ и сейчасъ же напрашивается опредѣленный выводъ. Получается благодарная почва для успѣшныхъ заключеній, сопоставленій и открытій, и не спасетъ тутъ даже и „раціональный" шифръ.

Если при этомъ еще производятъ сокращенія: ул. д. кв. (съ точками) и, вмѣсто прописи, пишутъ номеръ дома и квартиры цифрами, то дѣло становится еще проще (ср. гл. XVIII). Но если точекъ и не ставятъ, то все же поле для сопоставленій остается, хотя и значительно суженное.

Очевидно, для записыванія адресовъ нужны особые пріемы:

а) Названіе *города* не нужно помѣщать въ началѣ. Если его можно запомнить, то лучше вовсе не заносить, въ противномъ случаѣ его надо поставить гдѣ-нибудь въ серединѣ.

б) Въ названіи *улицы* незачѣмъ писать окончаніе „ая" или „ская". Фамилію адресата не нужно писать въ дательномъ падежѣ (напр., Эртелю).

в) Слова „улица", „домъ", „квартира", „для", „до востребованія" должны быть выброшены вовсе; способъ писанія адресовъ—какъ въ телеграммахъ: „Казанс Самара графа Шувалова третья Эртель Саша". Если же приходится сохранять *для себя* много адресовъ, причемъ благодаря обилію фамилій и подробностей можетъ произойти путаница, то тогда можно замѣнить эти слова условными обозначеніями, которыя должны быть различны въ разныхъ адресахъ, для чего лучше всего пользоваться видовыми названіями какого-нибудь рода, напр., растеній, звѣрей и т. п.

г) Нумера дома и квартиры можно и не зашифровывать (если только пишешь для *себя*), а писать цифрами, но помѣщать ихъ надо въ концѣ адреса и лучше извѣстнымъ, условнымъ образомъ измѣнивъ (т. е. увеличивъ или уменьшивъ): напр.: Дзика Варшава Брантъ Лиза $^{23}/_{5}$, вмѣсто: Варшава Дзикая улица д. № 20 кв. № 5 Бранту для Лизы. (Нумера условно увеличены на три).

д) Что касается замѣтокъ: „въ двухъ конвертахъ", „для явки", „для заказныхъ" и т. п., то ихъ можно и не зашифровывать, а надписывать ихъ сбоку обыкновенными буквами,—либо полностью, либо начальными буквами.

Необходимо имѣть въ виду, что если у кого-нибудь захваченъ списокъ адресовъ, зашифрованныхъ безупречно, но жандармамъ уже извѣстенъ какой-нибудь изъ нихъ (благодаря ли перехваченному письму по этому адресу или по какой-нибудь другой причинѣ), то у нихъ имѣется возможность добраться и до остальныхъ. Отсюда можно только вывести и безъ того понятное правило, что списки адресовъ, хотя бы хорошо зашифрованныхъ, надо прятать такъ основательно, чтобы они никоимъ образомъ не были найдены при обыскахъ.

2) *Походный (временный) шифръ.* Часто приходится давать адресъ для сношеній наскоро, второпяхъ, передъ отъѣздомъ. Собесѣдникъ X записываетъ его у себя на бумажкѣ или въ записной книжкѣ, чтобы послѣ зашифровать на досугѣ, а тотъ уѣзжаетъ, не зная о томъ, что станется съ даннымъ имъ адресомъ: будетъ ли онъ зашифрованъ, или нѣтъ, по хорошей ли системѣ или плохой. Можетъ также случиться, что прежде чѣмъ X соберется привести адресъ въ надежный видъ, къ нему придутъ съ обыскомъ. Ясно, что никто не имѣетъ права давать адресъ иначе, какъ съ тѣмъ, чтобы онъ тутъ же былъ зашифрованъ. Но при обыкновенныхъ системахъ (также и при „раціональной") это крайне затруднительно, ибо составленіе таблички требуетъ времени. Поэтому каждый революціонеръ долженъ обладать исключительно *для себя*, для временныхъ, короткихъ записей, такъ сказать походнымъ шифромъ. Его основнымъ качествомъ должна быть простота, бѣдность знаковъ, а потому легкая запоминаемость. Для этого можетъ служить либо единозначный шифръ, упрощенный до 12 паръ, либо квадратный изъ 5×5 клѣтокъ. Азбуку надо взять тюремную, сокращенную на 4 буквы для первой системы и на 3 для второй.

На таблицѣ № 71 изображена обыкновенная тюремная табличка для перестукиванія, пріобрѣвшая широкое распространеніе, на таблицѣ № 72—упрощенная табличка изъ 5×5 для квадратнаго походнаго шифра. Разница заключается въ томъ, что отсутствуетъ шестой горизонтальный рядъ и соотвѣтственно этому измѣненъ пятый; первые же четыре ряда тождественны; выброшены буквы ч, щ, ю, причемъ первая замѣняется посредствомъ *ц*, вторая посредствомъ *ш*, третья—*шу*. На табличку наносятъ два пятибуквенныхъ распредѣлителя, для которыхъ ключомъ можетъ слу-

жить какое-нибудь слово, напр.: „благодарность“. Въ немъ отдѣляютъ двѣ грани по пяти буквъ и производятъ по обыкновенному способу нумерацію:

б	л	а	г	о	д	а	р	н	о	сть
2	4	1	3	5	2	1	5	3	4	

Таблица № 71.

	1	2	3	4	5
1	а	б	в	г	д
2	е	ж	з	и	к
3	л	м	н	о	п
4	р	с	т	у	ф
5	х	ц	ч	ш	щ
6	ы	ю	я		

Таблица № 72.

	2	4	1	3	5
2	а	б	в	г	д
1	е	ж	з	и	к
5	л	м	н	о	п
3	р	с	т	у	ф
4	х	ц ч	ш щ	ы	я

Значенія буквъ на такой табличкѣ чрезвычайно легко заучить наизусть, какъ это и дѣлаютъ заключенные въ тюрьмахъ, прибѣгающіе при перестукиваніи къ шифрованнымъ табличкамъ. А тогда шифрованіе производится такъ же быстро, какъ и обыкновенное письмо.

Чтобы пользоваться единозначнымъ шифромъ, выбрасываемъ изъ тюремной азбуки, кромѣ вышеупомянутыхъ буквъ, еще букву *ф*, которую въ случаѣ нужды можно замѣнить посредствомъ „хв“, и беремъ слово изъ 12 различныхъ буквъ нашей упрощенной азбуки. Въ остальномъ поступаемъ какъ и при обыкновенномъ единозначномъ парномъ шифрѣ (гл. II). Напр.:

о б ы в а т е л в и ц у
г д ж з к м п р с х ш я

Адресъ наносится по возможности сокращенно; городъ не обозначается, номера пишутся въ концѣ въ измѣненномъ (условно) видѣ. Напримѣръ, адресъ: „Петербургъ Большая Морская 17 кв. № 5 Ивану Алексѣевичу Рыбникову“ мы изобразимъ такъ:

1) По таблицѣ № 72:

24535254533234132122521534123243245143155321, 13, 9

2) По единозначному парному:

дгртглнхзкранплждсхагз, 13, 9,

что значитъ: болморсивалксерыбников 13, 9

Нумера здѣсь измѣнены такъ, что первый уменьшенъ на 4, второй увеличенъ на столько же.

Такимъ же образомъ заносятся временно пароли, фамиліи и т. п. Однако, не позже того же вечера записи обязательно должны быть записаны по надежному ключу.

3) *Адресаты.* Какъ бы заботливо мы ни прятали наши адреса отъ глазъ жандармовъ, мы все же принуждены бываемъ выносить ихъ на свѣтъ божій и пускать открыто въ міръ на встрѣчу всѣмъ случайностямъ. Это происходитъ неизбѣжно съ адресами для почтовыхъ отправленій, писемъ, посылокъ, денегъ, телеграммъ и т. п., ибо ихъ приходится писать обыкновенными буквами, чернымъ по бѣлому, на конвертахъ, холстѣ, переводахъ, телеграфныхъ бланкахъ. Адресатъ есть, такимъ образомъ, первый козелъ отпущенія, первая мишень, куда устремляются удары жандармовъ; на немъ отражаются прежде всего всякаго рода промахи, допущенные отправителемъ. Съ другой стороны, отъ удачнаго выбора адресатовъ зависитъ въ громадномъ большинствѣ случаевъ, если не всегда, дойдетъ ли почтовое отправленіе благополучно или возбудитъ подозрѣніе и будетъ вскрыто. Такимъ образомъ, вопросъ о томъ, чьими адресами можно пользоваться, является вопросомъ очень серьезнымъ. Въ теоріи онъ давно уже рѣшенъ, хотя на практикѣ допускаются часто чреватыя дурными послѣдствіями отступленія, которыя иногда объясняются просто невозможностью осуществить требованія теоріи. Эта

послѣдняя заключается въ томъ, что адресаты должны быть люди безусловно „чистые", неизвѣстные жандармамъ, не участвующіе въ движеніи*). Не трудно понять громадныя преимущества, которыя доставляетъ такой выборъ. Во первыхъ, письмо при такомъ условіи имѣетъ несравненно больше шансовъ не возбудить подозрѣній и дойти благополучно. Революціонеровъ сравнительно немного и они тонутъ въ десяткахъ милліоновъ стоящихъ въ сторонѣ и не принимающихъ активнаго участія въ движеніи; они къ тому же почти всѣ либо уже отмѣченные „недреманнымъ окомъ", либо принадлежатъ къ „неблагонадежнымъ" профессіямъ и званіямъ: студенты, акушерки, учителя, статистики и т. п. Во вторыхъ, если бы, несмотря на такое благопріятное обстоятельство, письмо все же было вскрыто и затѣмъ послѣдовалъ обыскъ у адресата, то онъ не далъ бы никакихъ результатовъ въ смыслѣ нахожденія документовъ, литературы, посѣтителей революціонеровъ и такимъ образомъ остался бы безвреднымъ для организаціи и для дѣла. Совсѣмъ иное можетъ, конечно, оказаться, если адресатъ, много ли, мало ли, а принимаетъ участіе въ движеніи: тутъ всегда можетъ выйти очень непріятный сюрпризъ. Надо хорошо помнить, что вполнѣ надежный адресъ можетъ провалиться вслѣдствіе какой нибудь случайности или неблагопріятнаго стеченія обстоятельствъ. Сплошь и рядомъ бываетъ, что отправитель арестовывается на улицѣ или вокзалѣ въ то время, какъ онъ идетъ опускать письмо въ ящикъ; или къ нему приходятъ съ обыскомъ и находятъ у него только что изготовленное письмо съ надписаннымъ адресомъ; или вслѣдствіе грубаго недосмотра и небрежности письмо, посылка обращаютъ на себя вниманіе своимъ вѣсомъ, скверной упаковкой, просвѣчивающимъ содержимымъ и т. п.; или благополучно дошедшее уже письмо, доставленное отъ адресата къ получателю, находятъ у послѣдняго при обыскѣ вмѣстѣ съ конвертомъ; чаще всего это бываетъ съ открытками, ибо тутъ поневолѣ приходится отдавать текстъ вмѣстѣ съ адресомъ; или за отправителемъ слѣдятъ шпіоны и видятъ, какъ онъ опускаетъ письмо въ ящикъ, сдаетъ на почтѣ заказное, деньги, посылку, телеграмму. Словомъ, не можетъ подлежать сомнѣнію, что слѣдуетъ по возможности пользоваться адресами лицъ, непричастныхъ движенію. Но во всякомъ случаѣ мы должны считаться съ тѣмъ, что и самые надежные адреса могутъ провалиться, и что адресаты могутъ въ концѣ концовъ такъ или иначе пострадать, и вотъ тутъ является вопросъ, должна ли организація принимать такія жертвы; должна ли она, имѣетъ ли она право допускать, чтобы пострадалъ совершенно посторонній человѣкъ. Есть въ движеніи люди, которые рѣшаютъ этотъ вопросъ отрицательно: не должна, не имѣетъ права. Они разсуждаютъ такъ: мы пользуемся посторонними адресами, а не своими собственными не потому, чтобы мы хотѣли заставлять другихъ нести отвѣтъ за наши дѣйствія, чтобы мы желали прятаться за чужими спинами, а просто потому, что при этомъ меньше шансовъ проваливаться письмамъ и меньше вреда отъ перваго нападенія жандармовъ. Но разъ, тѣмъ не менѣе, фактъ совершился, разъ адресатъ взятъ—наша обязанность его выручить, что можетъ быть сдѣлано только такимъ путемъ, что получатель добровольно явится и признается въ своей роли. Нѣтъ сомнѣнія, что съ точки зрѣнія обыкновенной морали (конечно, высшаго калибра) такъ и должно бы было быть. Но совсѣмъ иное говоритъ рево юціонная мораль, мораль движенія въ цѣломъ. Она гласитъ, что не должно дѣлать того, что вредитъ интересамъ движенія, что играетъ на руку нашимъ врагамъ; если революціонеры будутъ добровольно отдаваться жандармамъ, чтобы тѣ не налагали наказанія на „невиннаго", то это будетъ, пожалуй, очень трогательно; но актомъ зрѣлаго сознательнаго бойца назвать это нельзя будетъ. Революціонерамъ не слѣдуетъ подражать „самоотверженному зайцу" въ извѣстной сказкѣ Салтыкова, тѣмъ болѣе, что жандармы могутъ поступить по рецепту щедринскаго волка. Похваливъ зайца, явившагося во время, чтобы выручить своего аманата, волкъ сказалъ: „Вижу, что зайцамъ вѣрить можно. И вотъ вамъ моя резолюція: сидите до поры-до времени, оба подъ этимъ кустомъ, а впослѣдствіи я васъ... ха-ха... можетъ быть помилую!"

Отношенія къ адресатамъ должны быть организованы такъ, чтобы послѣдніе не могли вредить получателямъ и въ то же время сами мало пострадали. Это можетъ быть достигнуто тогда, когда адресатъ 1) не знаетъ квартиры получателя и по возможности его настоящей фамиліи, и 2) когда получатель ходитъ за письмами къ адресату. Въ этомъ случаѣ послѣдній не можетъ фактически предать получателя,

*) Еще лучше, если это почтенные обыватели съ извѣстнымъ общественнымъ положеніемъ.

даже еслибы и хотѣлъ это сдѣлать, а съ другой стороны—его невинность такъ будетъ бить въ глаза, что его, конечно, долго держать не будутъ. Жандармы, само собой понятно, постараются поэтому дѣйствовать такъ, чтобы выслѣдить получателя. Узнавъ, что по такому-то адресу направляются нелегальныя письма, они не придутъ сейчасъ же съ обыскомъ, а раньше устроятъ надзоръ. Идущій за корреспонденціей долженъ всегда это имѣть въ виду и принимать всякій разъ такія предосторожности, какія должны практиковаться при посѣщеніи опасныхъ пунктовъ, ибо онъ не гарантированъ, что его не заберутъ тутъ же на улицѣ съ добычей въ карманѣ. Онъ не долженъ брать съ собой паспорта съ заявкой, чтобы по ней не могли сразу отправиться на его квартиру, гдѣ могутъ наткнуться на посѣтителей и такимъ образомъ сразу увеличить число жертвъ. На самой квартирѣ все должно быть чисто; если же этого нѣтъ, то онъ долженъ въ теченіе нѣкотораго времени скрывать свою квартиру. Въ его карманахъ не должно быть ни собственныхъ визитныхъ карточекъ, ни писемъ, хотя бы и легальныхъ, ни тому подобныхъ документовъ.—На конвертахъ нужно избѣгать писать „для N", „съ передачей N", ибо это выдѣляетъ письмо изъ множества другихъ. Вмѣсто этого лучше прибѣгать къ двумъ конвертамъ, но наличность внутренняго конверта не должна быть замѣтна снаружи. Почеркъ на конвертѣ никоимъ образомъ не долженъ быть ненатуральный, но все же надо писать такъ, чтобы нельзя было узнать почерка писавшаго. Въ особенности это надо имѣть въ виду при разсылкѣ по городской почтѣ воззваній.

Въ случаѣ, если сразу пишутъ нѣсколько писемъ, полезно разнообразить формы конвертовъ, цвѣтъ, величину, манеру писанія адреса и т. п.; внѣшность ихъ должна соотвѣтствовать адресатамъ: дамамъ—маленькіе, изящные; дѣловымъ людямъ—большіе, рабочимъ — попроще.

4) *Оказіи.* Многіе думаютъ, что если посылаютъ письмо не по почтѣ, а черезъ оказію, то допустимо отказаться отъ обычныхъ мѣръ предосторожности, напр. отъ шифра. Между тѣмъ, это глубокая и крайне вредная ошибка. За оказіей зачастую слѣдятъ и она можетъ быть арестована въ пути; сверхъ того нерѣдко вообще случайно останавливаютъ людей и обыскиваютъ (особенно на границѣ и въ пограничныхъ губерніяхъ). Наконецъ, уже по прибытіи посланца на мѣсто, привезенное имъ письмо обыкновенно странствуетъ черезъ многія руки, пока будетъ передано по назначенію, а, слѣдовательно, имѣетъ много шансовъ застрять гдѣ-нибудь, попасться при обыскѣ или въ лучшемъ случаѣ быть прочитаннымъ непосвященными людьми. Въ виду всего этого письма черезъ оказіи должны писаться совершенно такъ же, какъ и по почтѣ; адресъ получателя *никоимъ образомъ* не долженъ писаться на конвертѣ, а запоминаться оказіей, или если она не расчитываетъ на свою память, быть зашифрованнымъ на отдѣльной бумажкѣ. Не слѣдуетъ даже писать шифромъ открыто, ибо при случайномъ обыскѣ такое шифрованное письмо является вполнѣ вѣской причиной для ареста.

Къ великому стыду, мы должны признать, что сплошь и рядомъ лицо, везущее литературу, имѣетъ у себя въ карманѣ писанный, не шифрованный адресъ лица, которому надо передать литературу. Немало уже было, благодаря этому, проваловъ.

5) *Тюремная переписка.* Тюремная переписка гораздо опаснѣе, чѣмъ всякая другая, и это по весьма многимъ причинамъ. Прежде всего, такія записки имѣютъ несравненно больше шансовъ попасться въ руки жандармовъ. Если онѣ доставляются черезъ посредниковъ, то на первомъ планѣ надо всегда имѣть въ виду предательство. Во многихъ тюрьмахъ сами надзиратели предлагаютъ свои услуги заключеннымъ и потомъ прямехонько доставляютъ переписку въ жандармскія управленія. Также и уголовные арестанты частенько зарятся на ожидаемую награду. Все это долженъ имѣть въ виду заключенный и въ такихъ случаяхъ, прежде чѣмъ лѣзть въ воду, основательно пощупать почву подъ ногами. Извѣстный случай въ Кіевѣ, когда надзиратель доставилъ записку по начальству и за это удостоился торжественной похвалы и награды съ опубликованіемъ въ приказѣ, есть лишь одинъ изъ многихъ сотенъ аналогичныхъ. То же было въ Москвѣ въ полиц. части и въ Губернской тюрьмѣ. Въ Уфѣ арестованная Р. послала черезъ надзирателя шифрованную записку. Тотъ доставилъ ее начальству. Жандармы прочли и отправили ей отвѣтъ черезъ того же надзирателя. Завязалась оживленная переписка. Когда Р. узнала объ этой продѣлкѣ, она съ отчаянія чуть съ ума не сошла. Иногда же несчастный результатъ является слѣдствіемъ не предательства, а неумѣлости, неосторожности посредниковъ, строжай-

шаго надзора, которому подвергаются, какъ арестованный, такъ и всѣ соприкасающіяся съ нимъ лица. Если же письменныя сношенія совершаются безъ посредниковъ, то еще болѣе расширяется поле для все озможнаго рода несчастныхъ „случайностей", о которыхъ мы писали въ введеніи и которыя по праву должны быть названы „неизбѣжностями". Мы ихъ, по понятнымъ причинамъ, не станемъ перечислять здѣсь. Если прибавить къ этому, что самый процессъ писанія записки можетъ быть подсмотрѣнъ ретивыми церберами, что внезапные оффиціальные обыски и весьма частыя тайныя обшариванія камеръ (во время прогулокъ, допросовъ и т. п.) могутъ открыть уже приготовленныя или полученныя уже записки, что таковыя иногда забываются по небрежности въ библіотечныхъ книгахъ, въ карманахъ пальто и т. д. и т. д., то понятно станетъ, почему такой большой процентъ тюремныхъ записокъ не доходитъ по назначенію и частью попадаетъ въ руки жандармовъ. Когда записка такъ или иначе, обыкновенно безъ вѣдома обоихъ корреспондентовъ, попала во вражьи руки, то установить личность автора и адрес та дѣло чрезвычайно легкое. При ограниченности числа сидящихъ, если даже не указанъ прямо номеръ камеры получателя и нѣтъ подписи отправителя, почеркъ, а, главное, содержаніе записки сейчасъ же ихъ выдастъ. Можно себѣ представить, какъ рады бываютъ жандармы подобной добычѣ. Въ то время, какъ они изъ силъ выбиваются, чтобы получить какія-нибудь улики противъ арестованныхъ, установить ихъ знакомство, показать, что они причастны къ революціонному дѣлу, въ то время, какъ они зачастую не имѣютъ противъ нихъ никакихъ реальныхъ данныхъ, кромѣ глубокомысленныхъ соображеній, составленныхъ на основаніи невѣжественныхъ, извращенныхъ, мало уясняющихъ шпіонскихъ показаній,— они вдругъ получаютъ документы, изъ которыхъ они могутъ вывести очень много пріятныхъ вещей. По тону письма они заключаютъ о знакомствѣ; если тамъ есть шифрованныя фразы—значитъ, нар дъ опытный, изъ „настоящихъ" революціонеровъ. Но какова же ихъ радость, если въ перехваченныхъ запискахъ корреспонденты дѣлятся своими соображеніями, высказываютъ предположенія, уславливаются относительно показаній! „Если спросятъ про №№ (имя рекъ), скажите то-то". —„Боюсь, какъ бы не добрались до X (имя рекъ), тогда я пропалъ". — „Если откроется мое участіе въ праздникѣ, то я скажу...". Такія и подобныя блещущія наивностью фразы открываютъ жандармамъ цѣлый рядъ оставшихся имъ неизвѣстными обстоятельствъ, фактовъ, лицъ. Въ одной перехваченной запискѣ на волю сообщается, что на квартирѣ остался неоткрытымъ тайникъ съ важными документами, и въ результатѣ такой глупости—благополучно ускользнувшій было отъ глазъ сыска тайникъ попадаетъ въ его руки. Другой пренаивно сообщаетъ про невѣжество жандармовъ, которые обвиняютъ его въ томъ-то, тогда какъ на самомъ дѣлѣ онъ сдѣлалъ то-то. Вообще перехваченныя тюремныя записки составляютъ часто самый цѣнный матеріалъ въ рукахъ обвинителя.

Ясно, слѣдовательно, что въ тюремной перепискѣ требуется сугубая осторожность и специфическіе пріемы.

1. Желательно, чтобы личности корреспондентовъ по возможности не были констатированы, для этого надо:

а) Писать безъ всякаго обращенія и безъ подписи;

б) Печатными буквами;

в) О себѣ писать въ третьемъ лицѣ; точно также о личности адресата писать, какъ о третьемъ;

г) Можно обозначить всѣхъ участниковъ „дѣла" номерами, такъ чтобы они въ запискахъ фигурировали каждый подъ своимъ номеромъ. Но разумѣется, когда о комъ-нибудь изъ нихъ сообщается фактъ, извѣстный жандармамъ, то надо употребить его фамилію или истинные иниціалы. Напр., „Сегодня былъ допросъ у Маркова. Спрашивали то-то, показалъ то-то. Знакомства съ Ивановымъ, Петровымъ не призналъ. № 5 кланяется и сообщаетъ, что написалъ № 3. Получилъ ли № 8 (самъ адресатъ) записку отъ № 2 (самъ отправитель)", и т. д.;

д) Стараться по возможности, чтобы на запискахъ не были обозначены фамилія или номеръ камеры адресата.

2. Слѣдуетъ принять мѣры, чтобы переписка не имѣла вредныхъ послѣдствій. Для этого:

а) Тонъ письма долженъ быть сухой, оффиціальный;

б) Лицамъ, относительно которыхъ жандармамъ ничего неизвѣстно, шифрованныхъ записокъ, особенно въ первый періодъ заключенія. не посылать;

в) Самое важное для арестованныхъ — это быть au courant слѣдствія: знать, кто арестованъ, что найдено, о чемъ спрашиваютъ и какъ держатся на допросахъ. Зная, что извѣстно жандармамъ, выводятъ, что имъ осталось неизвѣстнымъ. Весь этотъ весьма важный, весьма необходимый матеріалъ можно сообщать совершенно открыто, безъ всякаго шифра. Дѣлиться же предположеніями, соображеніями рискованнаго свойства—совершенно излишне. Это допустимо только въ очень важныхъ случаяхъ;

в) Полезно писать о себѣ, какъ о человѣкѣ постороннемъ, къ дѣлу не причастномъ.

3. Все, что неизвѣстно и не должно стать извѣстнымъ жандармамъ, разъ объ объ этомъ необходимо снестись, слѣдуетъ обязательно и тщательно зашифровать, система должна быть безукоризненна. Книжный шифръ здѣсь совершенно непримѣнимъ, ибо книга, служащая ключомъ и по необходимости находящаяся у обоихъ корреспонтовъ, конечно, сейчасъ же станетъ извѣстной.

Кстати напомнимъ, что при устныхъ сношеніяхъ въ тюрьмѣ, громкихъ разговорахъ, перестукиваніи тоже необходимо соблюдать осторожность. Намъ извѣстны случаи арестовъ на основаніи подслушанныхъ разговоровъ. Для секретныхъ сообщеній надо употреблять шифрованную табличку, въ родѣ табл. № 72*).

Приложеніе.

РАЗНЫЕ СОВѢТЫ.

Предыдущей главой мы закончили поставленную себѣ задачу. Наша цѣль была разсмотрѣть существующія формы письменныхъ сношеній между революціонерами, показать ихъ недостатки и изыскать способы сдѣлать ихъ раціональными. Здѣсь же мы хотимъ заглянуть, хотя бы самымъ поверхностнымъ образомъ, въ другія сферы революціонной практики и отмѣтить важнѣйшіе изъ тѣхъ промаховъ, которые допускаются сплошь и рядомъ частью по халатности, частью по незнанію.

Квартира. 1) При наймѣ квартиры, хотя бы только для простого жительства, надо всегда обращать вниманіе, насколько изолирована она отъ сосѣдей: толсты ли стѣны, нѣтъ ли внутреннихъ дверей, куда выходятъ окна. У одного товарища окно квартиры выходило противъ довольно высокаго холма, и шпіоны забирались на скатъ вечеромъ и сквозь окно съ большимъ удобствомъ наблюдали за тѣмъ, что дѣлалось въ комнатѣ. Понятно, оцѣнка съ этой точки зрѣнія квартиры должна дѣлаться умѣло и дипломатично, чтобы не возбудить подозрѣнія у хозяевъ. Особенное же вниманіе и обдуманность нужно проявить при наймѣ квартиры для спеціальныхъ цѣлей: для собраній, для типографіи, склада и т. п.

2) Паспортъ нужно заявлять только тогда, когда этого невозможно больше откладывать или избѣгнуть. Всякая лишняя заявка на паспортѣ всегда неудобна. Опять таки и здѣсь не нужно проволочками возбудить какія-либо подозрѣнія у хозяевъ и дворниковъ.

3) Всегда надо имѣть въ виду, что многіе хозяева меблированныхъ комнатъ и весьма значительный процентъ дворниковъ состоятъ на жалованьи у тайной полиціи; въ особенности это практикуется въ университетскихъ городахъ.

---

*) Считаемъ необходимымъ сдѣлать здѣсь одно замѣчаніе, которое покажется крайне элементарнымъ, но которое, къ стыду нашему, сплошь и рядомъ оказывается нелишнимъ. Въ нѣкоторыхъ тюрьмахъ нерѣдко дѣлаются отступленія отъ строгихъ до нелѣпости правилъ, „инструкцій“: то не препятствуютъ переговариваться, то разрѣшаютъ переводить деньги на имя нуждающихся товарищей и т. д. Однако, заключенные чрезвычайно скоро сами портятъ свое положеніе тѣмъ, что пишутъ объ этомъ или другъ другу, или на волю; записки попадаются въ руки жандармеріи и она узнаетъ изъ нихъ о существующихъ „поблажкахъ“. Начинаются запросы; тюремное начальство получаетъ нахлобучку, и „льготы“ отнимаются. Отсюда ясно, что о всѣхъ подобныхъ вещахъ надо умѣть хранить полное молчаніе.

4) Не слѣдуетъ жить двумъ или нѣсколькимъ товарищамъ на одной квартирѣ: провалъ одного отражается такъ или иначе на остальныхъ сожителяхъ. До извѣстной степени допустимо жить совмѣстно съ мирнымъ обывателемъ, не „потрясающимъ основъ"; но надо имѣть въ виду, что въ случаѣ ареста будутъ допрашивать и сожителя, въ качествѣ свидѣтеля; и, конечно, онъ много зла можетъ принести своими простодушными и откровенными показаніями.

5) Какое бы довѣріе мы ни питали къ своей прислугѣ, къ хозяевамъ, сосѣдямъ, надо всегда имѣть въ виду, что въ случаѣ наше о ареста ихъ будутъ допрашивать, предъявлять имъ фотографическія карточки, застращивать и т. д. Мы не говоримъ уже о тѣхъ случаяхъ, когда они могутъ предать насъ неумышленно, по своей наивности. Поэтому надо принимать всѣ мѣры, чтобы окружающіе какъ можно меньше видѣли посѣтителей и совершенно не знали о конспиративной работѣ жильца.

6) Лучше всего устроиться такъ, чтобы квартира могла запираться нами при отлучкѣ изъ нея, а мѣстонахожденіе ключа было извѣстно 1—2 товарищамъ. Это дастъ возможность послѣднимъ, въ случаѣ внезапнаго нашего ареста внѣ квартиры (на улицѣ, собраніи, вокзалѣ и т. п.), очистить ее отъ всего компрометирующаго.

7) Если у себя дома занимаешься какой-либо нелегальной работой, то не надо забывать держать дверь на запорѣ, чтобы, при случайномъ посѣщеніи дворника, полицейскаго и т. п., имѣть возможность убрать подозрительное. Намъ извѣстно много проваловъ, происшедшихъ отъ несоблюденія этого элементарнаго правила. Одинъ товарищъ, напр., сидя у себя въ комнатѣ, писалъ прокламацію. Въ это время городовой принесъ какую-то бумагу, подъ которой нужно было расписаться. Застигнутый врасплохъ товарищъ сдѣлалъ невольное движеніе, чтобы прикрыть свою рукопись. Это сейчасъ же привлекло вниманіе городового, и въ результатѣ было арестовано трое человѣкъ.

8) Непремѣнно надо уславливаться относительно сигнализаціи на случай ареста; не мѣшаетъ также пользоваться таковой для обозначенія, находимся ли мы дома или нѣтъ; это избавляетъ отъ лишняго хожденія другъ къ другу. Сигнализація въ квартирахъ у насъ, можно сказать, основательно забыта, и отсутствіе ея часто влечетъ за собой совершенно личнія жертвы. Въ Москвѣ въ маѣ 1902 г. было взято 12 чел. въ то время, когда они сходились на назначенную квартиру, чтобы оттуда выступить на демонстрацію. Хозяинъ квартиры былъ арестованъ наканунѣ, и никто изъ собиравшихся не подозрѣвалъ этого. Сигналы должны быть такого рода, чтобы объ нихъ не могли догадаться посторонніе, иначе жандармы, въ случаѣ ареста, поддѣлаютъ сигналъ. (См. объ этомъ „Подпольн. Рос." Степняка).

9) Слѣдуетъ почаще производить у себя самого самый тщательный обыскъ. Нѣтъ ничего хуже завалявшихся бумажекъ, могущихъ быть найденными при обыскѣ.

10) Не хранить у себя на квартирѣ различныхъ жидкостей, гектографскихъ чернилъ и т. п. вещей, служащихъ для нелегальныхъ цѣлей. Гдѣ есть возможность, держать ихъ въ замаскированномъ видѣ; также не хранить у себя спеціальныхъ руководствъ (по печатанію, приготовленію красокъ и пр.).

11) Съѣзжая съ квартиры, не надо передавать ее такимъ товарищамъ, которые посѣщали насъ раньше и были замѣчаемы хозяевами, ибо это устанавливаетъ между ими и нами явную связь. Если же мы хотимъ ее передать кому-нибудь, то необходимо, чтобы это былъ такой, который у насъ раньше не бывалъ, и чтобы онъ снялъ комнату самостоятельно, какъ будто по вывѣшенному объявленію.

12) Нашъ образъ жизни, наша внѣшность, платье и т. п. должны быть такіе, чтобы какъ можно меньше казаться странными.

Конспиративная квартира. 13) На конспиративной квартирѣ образъ жизни долженъ быть въ высшей степени обдуманный и выдержанный; не нужно засиживаться по ночамъ, пѣть революціонныхъ пѣсенъ, производить подозрительный шумъ, жить слишкомъ замкнуто; надо вести такой образъ жизни, который сообразенъ съ объявленной профессіей. Провалы нерѣдко происходили съ такой стороны, съ какой меньше всего ихъ ожидали; въ одномъ мѣстѣ, напр., жильцы возбудили у хозяевъ подозрѣніе, не занимаются ли они фабрикаціей фальшивыхъ монетъ.

14) Живущіе на конспиративной квартирѣ должны стараться попадаться какъ можно рѣже на глаза полиціи, чтобы, въ случаѣ случайнаго ареста кого-нибудь изъ нихъ внѣ дома, не могло быть обнаружено немедленно его мѣстожительство.

15) Съ этой же цѣлью — спасти конспиративную квартиру на случай ареста внѣ дома, — обитатели ея не должны носить съ собой паспорта съ явкой своего дома, равно и

другихъ документовъ, своихъ визитныхъ карточекъ и т. п. вещей, констатирующихъ ихъ личность.

16) Работъ, сопряженныхъ съ шумомъ, никоимъ образомъ нельзя производить ночью.

17) Пуще всего слѣдуетъ оберегать квартиру отъ заноса шпіоновъ. При первомъ появленіи таковыхъ надо какъ можно скорѣе и осторожнѣе перемѣнить квартиру.

На улицѣ. 18) Выходя изъ дому надо всегда имѣть въ виду возможность внезапнаго ареста на улицѣ и потому не держать при себѣ безъ спеціальной надобности ничего компрометирующаго.

19) Всегда имѣть въ виду шпіоновъ; однако провѣрять себя надо умѣло: не бросать безпокойныхъ взглядовъ, не оборачиваться грубо и демонстративно, а удостовѣряться другими способами: направляясь проходными дворами, пустынными переулками, вскакивая на ходу въ конки и проч.

20) Тактика шпіоновъ чрезвычайно разработана и разнообразна. Очень часто, напр., они передаютъ свою „дичь", за которой охотятся, изъ рукъ въ руки, отъ квартала къ кварталу, идутъ параллельными улицами, забѣгаютъ впередъ и проч. Поэтому, если въ теченіе всей дороги мы не замѣтили ни одной фигуры, которая бы слѣдила за нами отъ начала до конца, если подозрительныя личности, которыя привлекаютъ наше вниманіе, исчезаютъ, не слѣдуя за нами, — то это еще ровно ничего не доказываетъ. — Если намъ приходится посѣщать часто конспиративную квартиру, то хотя бы намъ удавалось во время пути замести слѣдъ и уходить отъ шпіоновъ, тѣмъ не менѣе они всякій разъ будутъ ближе къ цѣли, ибо станутъ подстерегать насъ на томъ мѣстѣ, гдѣ потеряли въ прошлый разъ; благодаря этому они скоро доберутся до таинственной квартиры. Это надо имѣть всегда въ виду и тщательно провѣрять себя, какъ въ началѣ, такъ и въ концѣ пути. — Въ важныхъ случаяхъ, когда намъ надо отправиться въ конспиративное мѣсто, и мы не довѣряемъ собственному наблюденію, мы должны поручить опытному и нескомпрометированному товарищу слѣдовать сзади на значительномъ разстояніи и убѣдиться, нѣтъ ли за нами слѣженія.

21) Шпіонами часто служатъ извозчики, лавочники, дворники, продавцы сельтерской воды, сѣмячекъ и т. п.

22) Никоимъ образомъ не слѣдуетъ ходить революціонерамъ по улицамъ вдвоемъ, а тѣмъ болѣе компаніей, также показываться совмѣстно въ общественныхъ мѣстахъ, театрахъ, садахъ; не слѣдуетъ также назначать другъ другу дѣловыя свиданія въ публичныхъ мѣстахъ, скверахъ, ресторанахъ.

23) Не носить открыто пакетовъ, тѣмъ менѣе ночью.

24) Надо всячески избѣгать вокзаловъ, также быть осторожными на почтѣ.

25) На улицахъ, при встрѣчѣ съ товарищами, никоимъ образомъ не слѣдуетъ съ ними раскланиваться.

26) Подъѣзжая къ дому, не слѣдуетъ останавливать извозчиковъ или соскакивать съ конки у самой квартиры.

Товарищи. 27) Близорукимъ не слѣдуетъ давать такихъ функцій, гдѣ возможны встрѣчи съ шпіонами; къ ихъ увѣреніямъ, что за ними не слѣдятъ, что все обстоитъ благополучно, надо относиться скептически.

28) Лишь только за кѣмъ-нибудь констатировано слѣженіе, его нужно немедленно и рѣшительно изолировать, оставляя въ сторонѣ всякія другія соображенія. Кто подъ вліяніемъ похвальнаго рвенія къ работѣ скрываетъ отъ товарищей или умаляетъ фактъ слѣженія, тотъ совершаетъ преступленіе.

29) Организація должна время отъ времени устраивать собственный надзоръ за своими членами, чтобы убѣдиться, насколько они конспиративны, и не слѣдятъ ли за ними шпіоны.

30) Не слѣдуетъ оставаться на ночь въ подозрительномъ мѣстѣ, за которымъ слѣдятъ. Въ февралѣ 1902 г. въ Елизаветградѣ 4 человѣка зашли къ одному рабочему, чтобы у него заночевать. Они застали его сжигающимъ кой-какую литературу, такъ какъ онъ ожидалъ у себя обыска. Гости его успокоили и остались ночевать. Въ ту же ночь всѣ пятеро были забраны на этой квартирѣ.

31) Не надо провожать уѣзжающихъ.

32) Не надо зря ходить другъ къ другу въ гости.

33) Заходя къ товарищу, слѣдить тщательно за условными сигналами, обращать вниманіе на подозрительныя особенности. Осторожность должна быть удвоена при посѣщеніи квартиръ въ чужомъ городѣ, проѣздомъ.

34) Зайдя къ товарищу и не заставъ его дома, не слѣдуетъ оставлять ему нелегальныхъ записокъ или вещей на столѣ или въ другомъ мѣстѣ. Подобные поступки много разъ вели къ роковымъ послѣдствіямъ. Въ Петербургѣ одинъ получилъ черезъ „оказію“ для передачи шифрованное письмо. Онъ понесъ его къ адресату и, не заставъ дома (тотъ жилъ въ меблированныхъ комнатахъ), положилъ письмо на столъ подъ скатерть. Тутъ же онъ написалъ „легальную“ записку, гдѣ онъ давалъ намекъ заглянуть подъ скатерть, и оставилъ ее открыто на столѣ. На другой день обезпокоившись онъ снова навѣстилъ адресата. Оказалось, что тотъ записку прочелъ, ничего не понялъ, и письмо по прежнему лежало подъ скатертью. Въ ту же ночь къ адресату совершенно неожиданно пришли съ обыскомъ, но ничего уже, конечно, не нашли. Письмо было такого рода, что еслибы оно попалось, то были бы обнаружены и лицо, писавшее его, и посредникъ.

35) Съ неизвѣстнымъ лицомъ, являющимся изъ другихъ мѣстъ, хотя бы по конспиративному адресу и съ условнымъ паролемъ, надо соблюдать величайшую осторожность. Первое время слѣдуетъ только распрашивать и ничего не разсказывать, сопоставлять его сообщенія, убѣждаться въ отсутствіи противорѣчій въ его разсказѣ и пр.

36) Для сокращенія взаимнаго хожденія можно иногда пользоваться телефонами (крайне осторожно), городской почтой, посыльными, конечно, съ соблюденіемъ соотвѣтственныхъ мѣръ.

37) Члены организаціи должны звать себя по кличкамъ, фиктивнымъ именамъ и фамиліямъ. Настоящая фамилія должна быть неизвѣстна. Но надо имѣть въ виду, что когда въ „обществѣ“ какое-нибудь лицо, не въ примѣръ прочимъ, слыветъ подъ кличкой, то это на него привлекаетъ вниманіе и можетъ имѣть дурныя послѣдствія. Не слѣдуетъ также звать по фамиліи подложнаго паспорта.

38) На калошахъ не нужно имѣть своихъ истинныхъ иниціаловъ. Это часто даетъ предателямъ нить для разысканія лицъ, фамиліи которыхъ имъ неизвѣстны.

„*Сборища*“. 39) Нельзя устраивать собраній, хотя бы и малолюдныхъ, на квартирахъ, гдѣ хранится литература или другія нелегальныя вещи.

40) На квартирѣ, гдѣ засѣдаетъ комитетъ или другое аналогичное учрежденіе, не должно быть никакихъ предметовъ, которые бы указывали на наличность засѣданія и какого именно, напр.: комитетской печати, писемъ и т. п. То же, что необходимо, всегда надо такъ расположить, чтобы можно было быстро уничтожить (напр., передъ топящейся печкой).

41) Отправляясь на многолюдное собраніе, нелегальную вечеринку, демонстрацію, праздникъ, вообще во всякое мѣсто, гдѣ имѣются шансы быть арестованнымъ, надо тщательно очистить свою квартиру, осмотрѣть карманы и запереть двери, чтобы никто изъ товарищей не могъ къ вамъ зайти и очутиться случайно во время обыска.

42) Для обезпеченія собраній отъ внезапнаго нападенія полиціи слѣдуетъ всегда разставлять часовыхъ, хотя бы эти собранія происходили на дому.

43) Возвращаясь съ загородныхъ собраній, надо расходиться въ одиночку, въ особенности не должны ходить рядомъ интеллигенты и рабочіе.

44) Во время засѣданій, собраній,—верхнее платье, калоши, палки не должно оставлять въ передней, чтобы при случайномъ посѣщеніи дворника или полицейскаго не видно было сразу, что происходитъ собраніе.

Поѣздки. 45) Самый опасный пунктъ при поѣздкахъ — вокзалъ, а въ особенности опасна процедура покупки билета. Тутъ слѣдуетъ быть особенно осторожнымъ.

46) Билетъ желѣзнодорожный надо брать нѣсколько дальше того пункта, куда ѣдешь, чтобы при арестѣ въ вагонѣ и отъ кондуктора нельзя было узнать конечный пунктъ путешествія.

47) Въ особо важныхъ случаяхъ надо остановиться въ какомъ-нибудь промежуточномъ пунктѣ для провѣрки, нѣтъ ли „хвоста“; измѣнять маршрутъ, ходить пѣшкомъ.

48) Ѣдущій на съѣздъ обязанъ послѣднее время передъ назначеннымъ срокомъ изолироваться отъ всякихъ дѣлъ и даже по возможности перемѣнить мѣстожительство и измѣнить наружность.

49) Никоимъ образомъ не надо заявлять во время съѣзда своего паспорта, такъ какъ эта заявка послѣ можетъ оказаться вполнѣ убѣдительной уликой. Надо также по возможности устроить такъ, чтобы отъѣздъ изъ дому остался незамѣченнымъ.

50) Во время объѣзда многихъ пунктовъ надо послѣ каждаго посѣщенія но-

ваго города провѣрять себя, не „зацѣпилъ“ ли шпіона. При малѣйшемъ подозрѣніи — принять самыя тщательныя мѣры, чтобы очиститься.

51) Если везутъ съ собой въ вагонѣ или багажемъ литературу, шрифтъ и т. п. вещи, то первымъ дѣломъ надо обратить вниманіе на то, чтобы корзина или чемоданъ не бросались въ глаза своей относительной тяжестью. Лучше поэтому большій объемъ при относительной легкости, чѣмъ небольшая, но тяжелая упаковка. Въ такихъ случаяхъ не нужно самому выносить изъ вагоновъ вещей, а поручать это носильщикамъ.

Смѣсь. 52) Скрывающійся отъ шпіоновъ въ другомъ городѣ долженъ помнить, что какъ бы далекъ ни былъ этотъ пунктъ отъ его прежняго мѣстожительства, онъ нисколько не гарантированъ отъ того, что его не узнаютъ. Шайка шпіоновъ уже давно стало „междугородней“. Поэтому не нужно показываться въ общественныхъ мѣстахъ, театрахъ, на вокзалѣ; избѣгать людныхъ улицъ, мало выходить днемъ.

53) Живущій нелегально долженъ чаще мѣнять паспорта.

54) Во время заявки фальшиваго паспорта — держать квартиру совершенно чистой и не разрѣшать никому ее посѣщать.

55) Обыскъ или арестъ на основаніи шпіонскаго слѣженія стоитъ въ различномъ временномъ соотношеніи къ этому послѣднему, въ зависимости отъ соображеній Департамента Полиціи. То слѣженіе продолжается очень долго, по цѣлымъ полугодіямъ, и кончается затѣмъ массовымъ проваломъ; то обыскъ и арестъ производится въ тотъ же день или ночь, какъ данная квартира или лицо возбудили противъ себя подозрѣнія шпіоновъ. Измѣнчивость этой тактики надо всегда имѣть въ виду. Лишь только фактъ слѣженія установленъ, надо немедленно принять мѣры: либо скрыться, либо очиститься и прекратить всякія сношенія съ организаціей.

56) Если за кѣмъ-либо началось слѣженіе и потомъ оборвалось, то можно быть увѣреннымъ, что впослѣдствіи при арестѣ старыя шпіонскія записи будутъ предъявлены, а если почему-нибудь не сочтутъ нужнымъ ихъ показывать, то, во всякомъ случаѣ, они пойдутъ въ „дѣло“.

57) На допросахъ не нужно признавать ничего ни за собой, ни за другими; не обращать вниманія на угрозы жандармовъ; не вѣрить ихъ заявленіямъ про другихъ, даже если они будутъ предъявлять собственноручные протоколы; имѣть въ виду, что показанія шпіоновъ весьма часто бываютъ крайне лживы, вслѣдствіе того, что они принимаютъ одно лицо за другое, ошибаются домомъ, этажомъ, квартирой и т. д.

58) Не давать и не брать ни у кого фотографическихъ карточекъ, не дѣлать на нихъ надписей, не держать у себя альбомовъ съ карточками.

59) Не держать у себя книгъ съ инициалами или фамиліями владѣльцевъ.

60) Нужныя вещи для гектографа, миміографа не слѣдуетъ покупать сразу въ одномъ мѣстѣ.

61) Никогда не слѣдуетъ отправлять посылокъ, денегъ, телеграммъ, заказныхъ по тѣмъ адресамъ, которые даны для простыхъ писемъ.

62) Отправляя телеграммы, слѣдуетъ помнить, что текстъ ихъ не уничтожается. Это надо имѣть въ виду какъ относительно содержанія, такъ и почерка.

63) Не нужно выбирать въ качествѣ адресатовъ своихъ родственниковъ, потому что въ случаѣ заполученія такого письма жандармы могутъ легко открыть писавшаго и такимъ образомъ схватить нить за оба конца.

64) Не нужно дѣлать помѣтокъ своимъ почеркомъ на поляхъ нелегальныхъ книгъ и газетъ.

65) Уничтожать письма, рукописи и т. д. лучше всего сжиганіемъ, стараясь при этомъ, чтобы не оставалось пепла.

66) Въ случаѣ ареста на улицѣ, задержки шпіономъ, дворникомъ, объѣздчикомъ, полицейскимъ — иногда бываетъ цѣлесообразно пустить въ ходъ деньги — средство, неоднократно оказывавшееся спасительнымъ для революціонеровъ.

А. Бундовецъ.

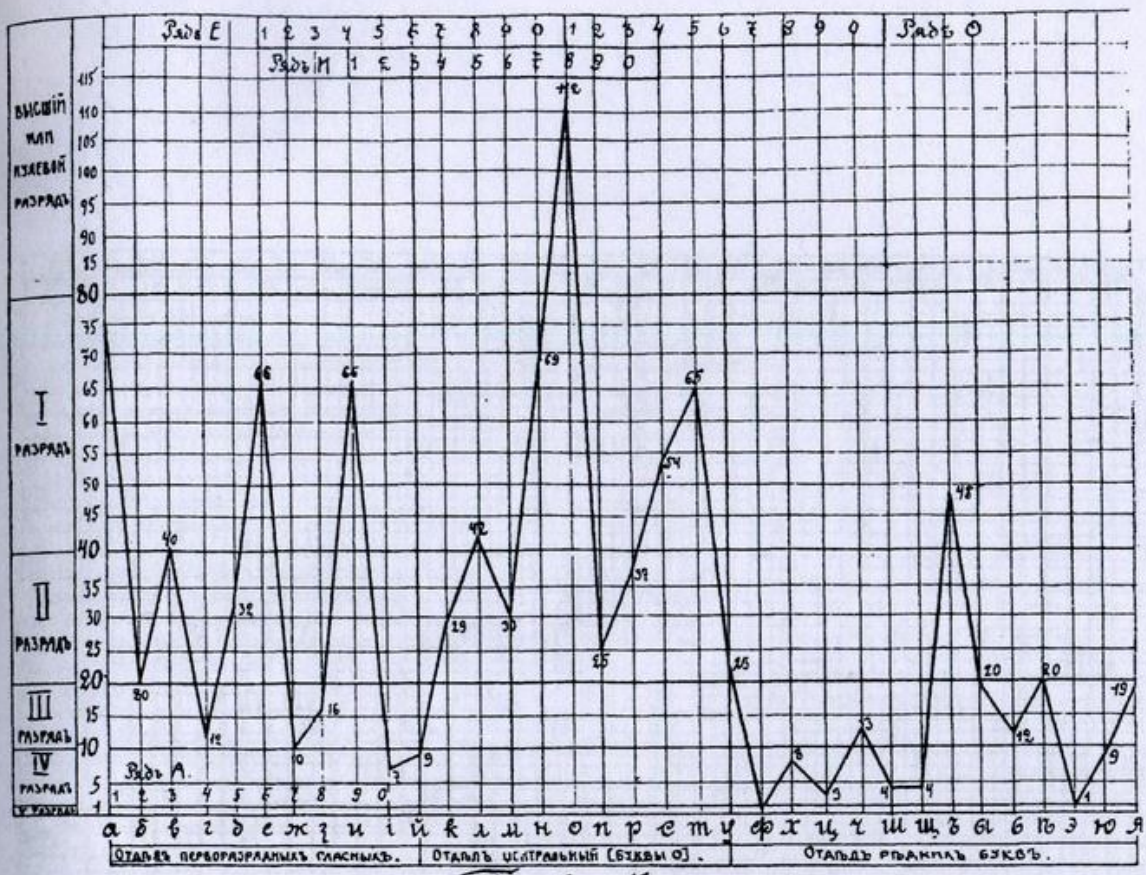


Табл. 5.

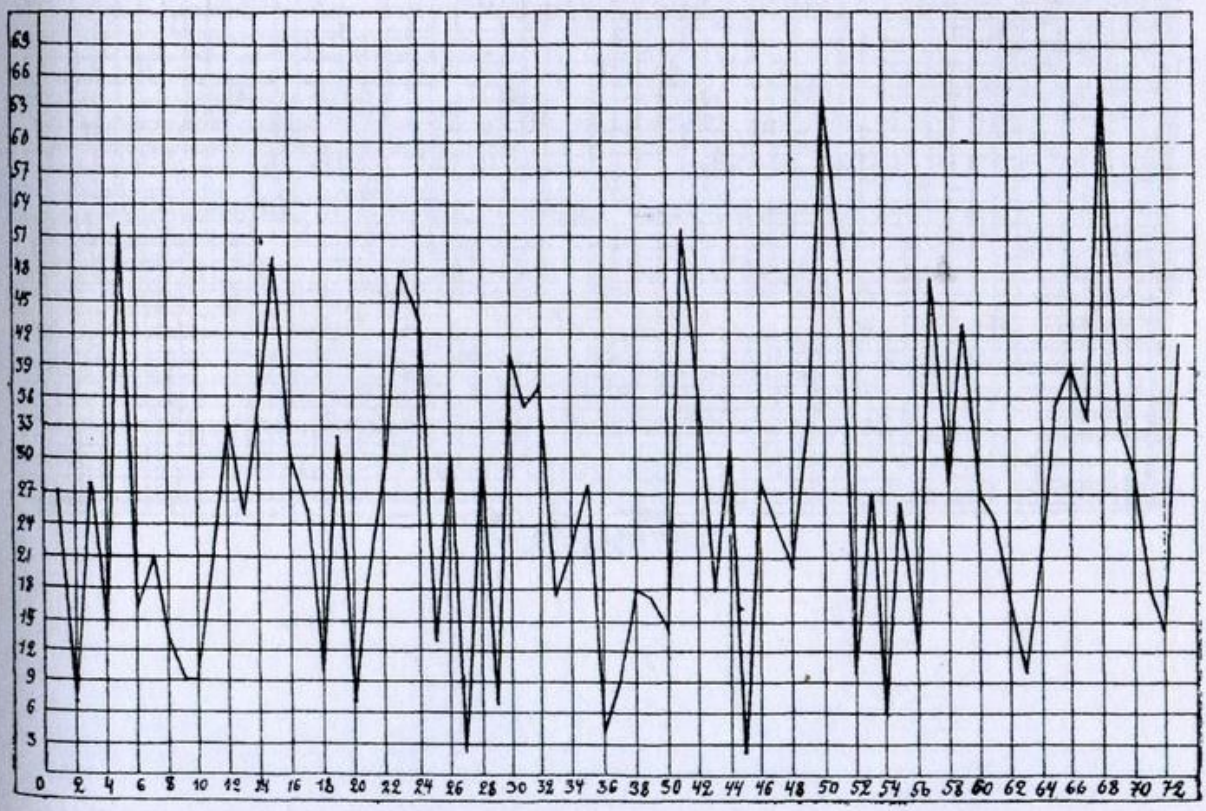
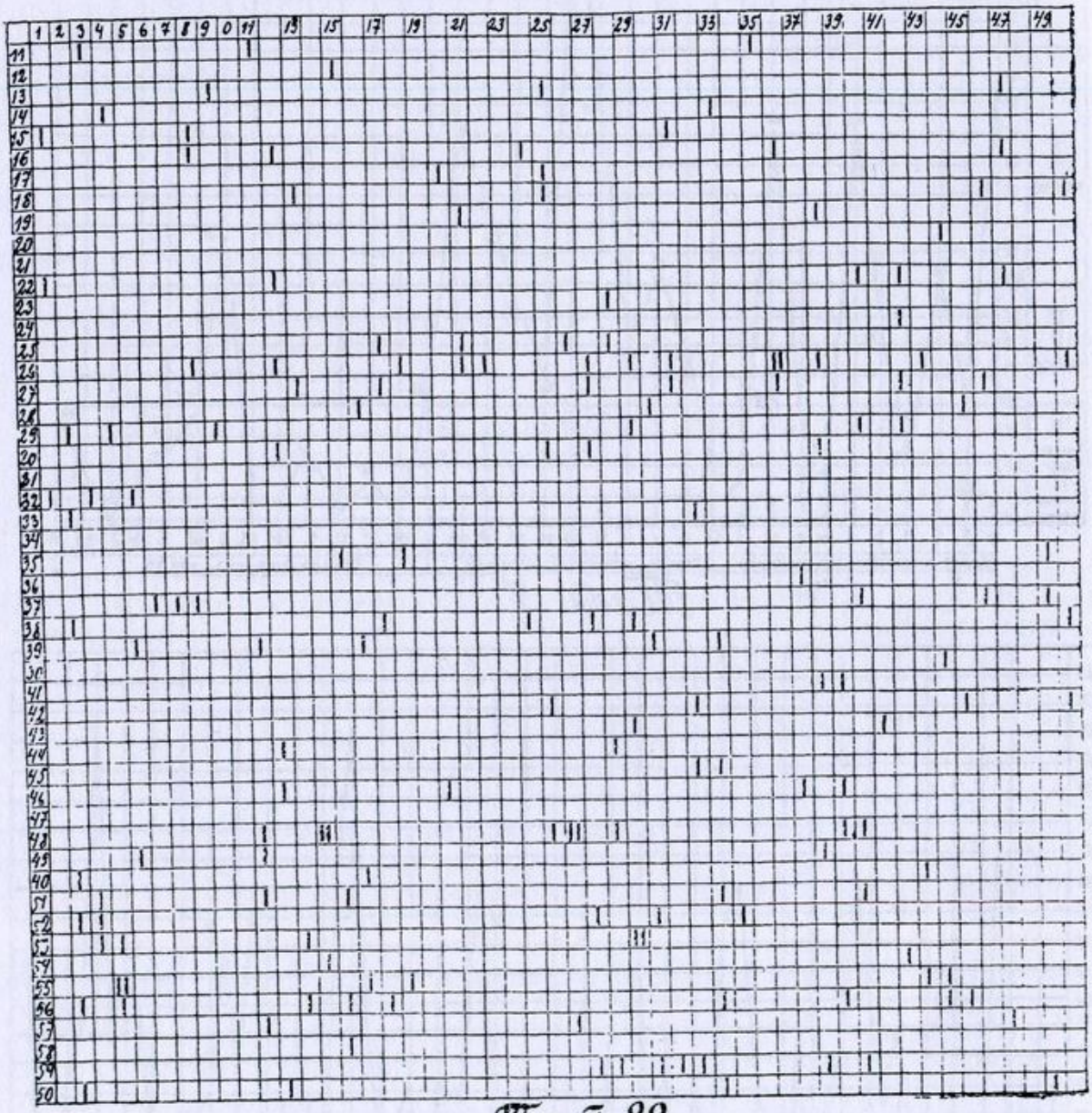


Табл. 35.



Таб. 29.

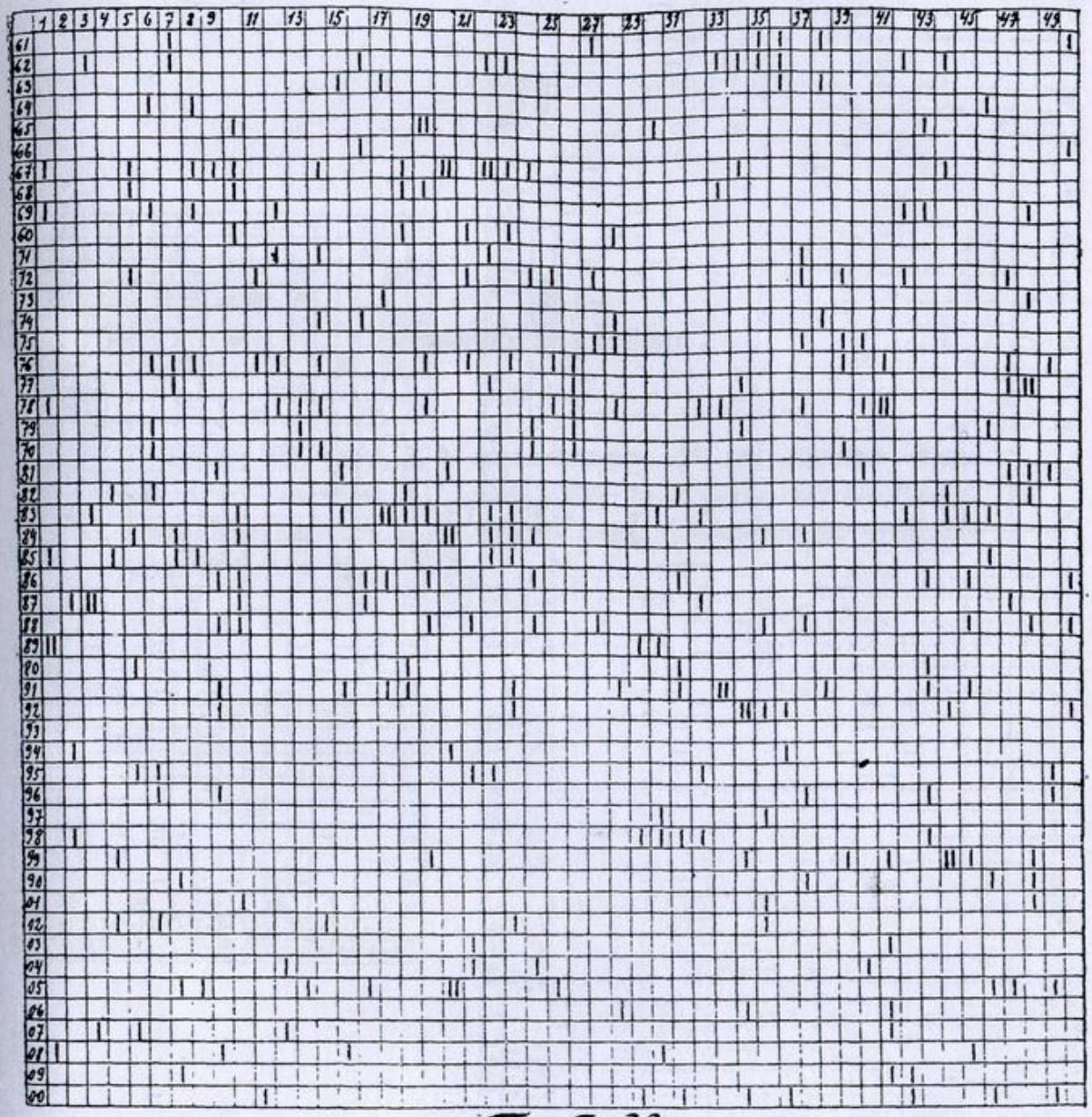
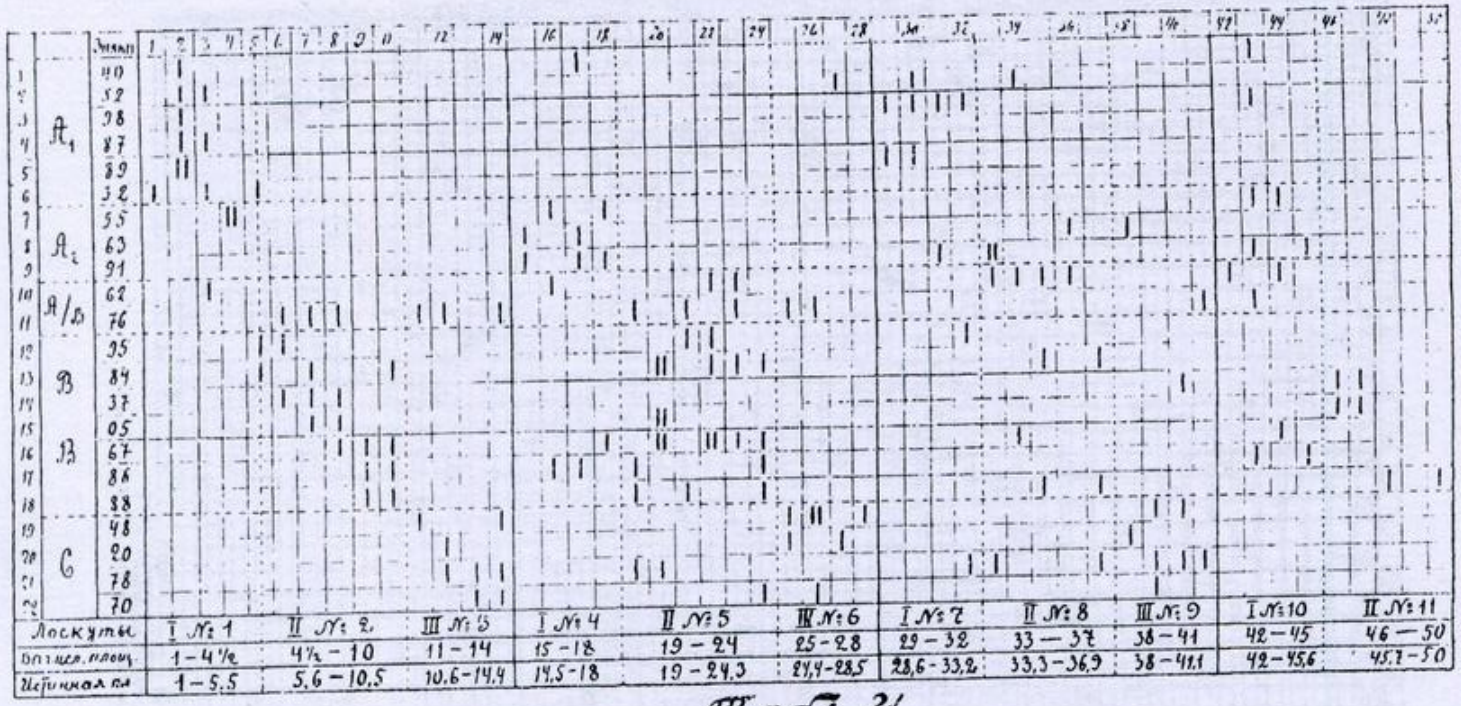
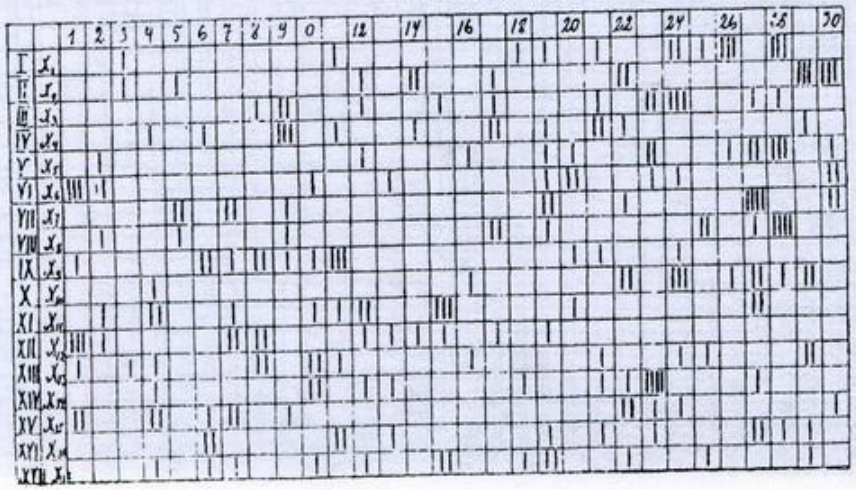


Табл. 30.


Эталон
A1
A2
A/Б
B
Б
C
Лоскутки
I № 1
II № 2
III № 3
I № 4
II № 5
III № 6
I № 7
II № 8
III № 9
I № 10
II № 11
1 – 4 1/2
4 1/2 – 10
11 – 14
15 – 18
19 – 24
25 – 28
29 – 32
33 – 37
38 – 41
42 – 45
46 – 50
1 – 5.5
5.6 – 10.5
10.6 – 14.4
14.5 – 18
19 – 24.3
24.4 – 28.5
28.6 – 33.2
33.3 – 36.9
38 – 41.1
42 – 45.6
45.7 – 50

Таб. 31



Замѣченныя опечатки.

На стр. 17, табл. № 2, *напечатано:* „56, ы“; *должно быть* „26, ы“. — На табл. № 29 (стр. 110), въ первомъ вертикальномъ столбцѣ (слѣва), въ 11-ой клѣткѣ (сверху) *изображено* число 20; *должно быть:* **10**.