ГЛАВА 15.

О чтеніи шифрованныхъ писемъ.

1. Общія замѣчанія.

Приступая къ изложенію способовъ прочтенія разнаго рода шифрованныхъ писемъ, я, конечно, долженъ ограничиться лишь самымъ необходимымъ, такъ какъ болѣе или менѣе исчерпывающій очеркъ потребовалъ бы отдѣльнаго и объемистаго тома. Тѣмъ не менѣе я надѣюсь изложить здѣсь все, что можетъ понадобиться С. С. въ его обыденной дѣятельности. Обращаясь къ вопросу о сущности шифра, слѣдуетъ различить шифръ въ собственномъ смыслѣ, употребляемый въ дипломатическихъ и высшихъ военныхъ сферахъ, и шифръ низшаго рода, употребляемый частными лицами съ серьезными и несерьезными цѣлями всякаго рода. Первый изъ нихъ примѣняется для сохраненія высшихъ государственныхъ тайнъ и сообщеній и важныхъ военныхъ донесеній и распоряженій и составляетъ рядъ болѣе или менѣе искусственныхъ сплетеній, разгадываніе которыхъ возможно для непосвященныхъ лишь въ очень рѣдкихъ случаяхъ. Для этого необходима особая подготовка, особый даръ и даже особое счастье: при недостаткѣ хотя бы одного изъ этихъ качествъ шифрованное письмо такимъ и останется.

Что касается простыхъ шифровъ, то разобрать ихъ можетъ всякій, который только обладаетъ терпѣніемъ, усердіемъ и, хотя отчасти, особымъ даромъ и счастьемъ. Въ этой главѣ я буду говорить исключительно о шифрѣ послѣдняго рода. Однако вовсе не такъ легко опредѣлить, что составляетъ шифръ простой и что шифръ искусственный, такъ какъ между депешей, шифрованной по различнымъ системамъ, съ примѣненіемъ разныхъ языковъ, и письмомъ, въ которомъ лишь переставлены буквы въ извѣстномъ

порядкѣ, можетъ быть еще множество шифровъ, съ большимъ или меньшимъ трудомъ разгадываемыхъ, такъ что провести различіе между труднымъ и легкимъ шифромъ нѣтъ возможности. Кромѣ того, трудность эта имѣетъ чисто субъективный характеръ. Простѣйшій шифръ представитъ огромнѣйшія затрудненія для человѣка неопытнаго и несмѣтливаго, тогда какъ спеціалистъ въ этой области, состоящій въ министерствѣ иностранныхъ дѣлъ или въ генеральномъ штабѣ, прочтетъ въ короткое время и вполнѣ правильно несомнѣнно запутанное и сложное шифрованное письмо.

Не требуетъ доказательствъ, что всякое обнаруживаемое при производствѣ слѣдствія шифрованное письмо представляется для С. С. въ высшей степени важнымъ, ибо уже самое примѣненіе лицомъ заподозрѣннымъ или тѣми, которые съ нимъ переписываются, тайныхъ письменныхъ знаковъ, указываетъ на желаніе ихъ скрыть что-либо отъ властей. Съ другой стороны, успѣшное прочтеніе такихъ писемъ обыкновенно разъяснитъ дѣло въ гораздо большей степени, нежели многочисленные допросы и обстоятельныя дознанія. Переписка посредствомъ шифра встрѣчается въ уголовныхъ дѣлахъ гораздо чаще, нежели обыкновенно думаютъ: слѣдуетъ только поискать, и кто потрудится разсмотрѣть бумаги, отмѣтки, письма и записки заподозрѣннаго и розыскать таковыя во всѣхъ его карманахъ, складкахъ и подшивкахъ его одежды, тотъ найдетъ множество такихъ письменныхъ записей, которыя, при ближайшемъ разсмотрѣніи, окажутся шифрованными. Такимъ будетъ и письмо, повидимому, безсмысленнаго содержанія, или какая нибудь непонятная «глупость», и каракули, кажущіяся на первый взглядъ лишенными всякаго значенія. И если такія сношенія обнаружены во время производства слѣдствія, то именно потому и слѣдуетъ обратить серьезное вниманіе на эти письма. Конечно, бываютъ и такіе случаи, когда цѣлыя пачки шифрованныхъ писемъ и записокъ не подвинутъ слѣдствія ни на шагъ, но никогда не слѣдуетъ опредѣлять это заранѣе: правильнѣе предположеніе, что такая находка можетъ повести къ какимъ нибудь послѣдствіямъ. Такъ напр., нахожденіе шифрованной записки у лица, заподозрѣннаго въ кражѣ серебряныхъ часовъ, даетъ по меньшей мѣрѣ основаніе заключить, что мы имѣемъ дѣло съ воромъ, изощрившимся въ своемъ дѣлѣ, съ членомъ воровской шайки и т. п.

Слѣдуетъ положить себѣ за правило,—всякое шифрованное письмо разбирать, по крайней мѣрѣ дѣлать къ тому попытки;—какимъ образомъ, конечно, иной вопросъ. Представляется ли дан-

ный шифръ простымъ или сложнымъ, на первый взглядъ почти никогда нельзя сказать. Есть такіе виды шифровъ, которые сначала кажутся чрезвычайно сложными (напр. шифры изъ однѣхъ гласныхъ буквъ), а затѣмъ безъ особаго труда разбираются. И наоборотъ, нѣкоторые шифры представляются наипростѣйшими, тогда какъ ихъ не въ состояніи распутать самое опытное въ этомъ отношеніи лицо.

Поэтому С. С., какъ только попадаетъ въ его руки шифрованное письмо, волей-неволей приходится самому попытаться его разбирать. При этомъ онъ можетъ руководствоваться или тѣми немногими указаніями, которыя излагаются ниже, или же, если у него окажется желаніе и соотвѣтствующія способности, заняться изученіемъ одного изъ тѣхъ руководствъ, которыя спеціально трактуютъ объ искусствѣ читать шифрованное. Тайнопись была извѣстна грекамъ и римлянамъ, а въ средніе вѣка, особенно въ XV столѣтіи, ею стали заниматься очень основательно. «Manuscript italien» 1595 французской національной библіотеки содержитъ напр. на стран. 438—446 отрывки: «Diario de Cicco Simonetta», секретаря и совѣтника трехъ первыхъ миланскихъ герцоговъ изъ династіи Сфорца,—въ которомъ приведены, Regulae ad extrahendum litteras zifferatas sine exemplo» (1474 г.). Впослѣдствіи появились полныя системы тайнописи, въ настоящее же время мы имѣемъ цѣлый рядъ учебниковъ по этому предмету. Какъ таковые, можно рекомендовать д-ра І. Людвиг. Клюбера «Kryptographia» (старое, но вполнѣ пригодное руководство, служитъ и до сего времени основаніемъ для всѣхъ позднѣйшихъ работъ по тому же вопросу и содержитъ обзоръ ранѣе вышедшей литературы предмета), Эдуарда Флейснера ф.-Востровичъ «Handbuch der Kryptographie» Вѣна, Ф. В. Казискаго «Die Geheimschriften und die Dechiffrierkunst», Берлинъ 1863, В. де-Романини «La Cryptographie dévoilée» Парижъ 1857 г. и др.

Пользуясь какимъ либо изъ этихъ руководствъ (я лично предпочитаю Флейснера, какъ наиболѣе практичное), при нѣкоторомъ усердіи и дарованіи можно съ успѣхомъ разбирать несомнѣнно сложные и трудные шифры. Правда, всегда, кромѣ того, нужно еще и счастье: благодаря какой-нибудь случайности можно добиться сразу того, чего не сдѣлаешь и въ теченіе нѣсколькихъ дней; но «случайность» эту слѣдуетъ подмѣчать и ею пользоваться. И здѣсь можно сказать то же, что мы говорили о всей дѣятельности С. С.: повидимому, успѣхъ его зависитъ отъ счастья, но въ дѣйствитель-

пости этотъ успѣхъ слѣдуетъ приписать расторопности и внимательности С. С., который съумѣлъ подмѣтить и воспользоваться этимъ «счастливымъ» оборотомъ обстоятельствъ. Кромѣ того, въ остальномъ отношеніи С. С. для разбора шифровъ долженъ имѣть доброе желаніе, нѣкоторое упорство, ревность къ дѣлу, зоркій взглядъ и способность къ комбинаціямъ,—т. е. всѣ тѣ качества, которыми вообще долженъ обладать С. С. Можно даже сказать такъ, что кто способенъ быть С. С., можетъ разбирать и шифрованное. Но если С. С. встрѣтитъ непреодолимыя препятствія въ прочтеніи шифрованнаго письма, то онъ можетъ обратиться или въ министерство иностранныхъ дѣлъ или въ военное. Хотя такого рода помощь и не лежитъ на обязанности этихъ министерствъ, тѣмъ не менѣе С. С. можетъ разсчитывать на ихъ содѣйствіе, если только прибѣгаетъ къ нимъ въ самыхъ крайнихъ случаяхъ.

Въ крупныхъ городахъ, впрочемъ, можно найти лицъ, свѣдущихъ по части разбора шифровъ: отставныхъ офицеровъ генеральнаго штаба, дипломатовъ, математиковъ и др. Тотъ, кому въ жизни пришлось заниматься этимъ дѣломъ, часто пріобрѣтаетъ такой интересъ къ нему, что съ охотой принесетъ свои познанія на пользу общую. Но такими лицами С. С., конечно, можетъ располагать лишь въ исключительныхъ случаяхъ, вообще же ему приходится разсчитывать только на свои силы. Слѣдуетъ добавить, что С. С. въ этихъ случаяхъ поставленъ въ болѣе выгодное положеніе, нежели дипломатъ или офицеръ генеральнаго штаба, которымъ по должности приходится разбирать шифры. Ни тотъ, ни другой въ большинствѣ случаевъ не знаютъ, на какомъ языкѣ написанъ шифръ, кто съ кѣмъ переписывается, о чемъ идетъ рѣчь и т. д. Онъ знаетъ только одно, что письмо написано съ величайшею тщательностью и съ примѣненіемъ самыхъ тонкихъ хитростей, отнюдь не облегчающихъ его труда. Дипломатъ или офицеръ генеральнаго штаба никакой помощи извнѣ не имѣютъ: вѣдь не случается, чтобы вмѣстѣ съ шифрованной депешей они получили и ключъ къ шифру. Другое дѣло, если таковой имъ указанъ, но тогда уже нельзя говорить о чтеніи шифровъ въ строгомъ смыслѣ слова.

У С. С. эта сторона дѣла, по крайней мѣрѣ въ большей части случаевъ, въ нѣкоторомъ отношеніи легче: получивъ шифрованное письмо, онъ почти всегда имѣетъ уже заподозрѣнное лицо, которое сочинило письмо, или то, которому оно предназначалось. Такимъ образомъ С. по меньшей мѣрѣ извѣстна степень ихъ образованія;

онъ можетъ предположить, на какомъ языкѣ составленъ шифръ и въ чемъ приблизительно содержаніе письма; по степени образованія субъекта онъ можетъ заключить и объ орфографіи писавшаго (что очень важно) и о томъ, какой родъ шифра онъ могъ избрать. И дѣйствительно, надо имѣть большое развитіе ума, чтобы съумѣть разобраться и примѣнить слишкомъ сложныя системы шифра. Чтобы привести себѣ въ ясность всѣ эти обстоятельства, С. С. неизбѣжно долженъ вновь съ этой точки зрѣнія просмотрѣть все слѣдствіе,—какъ это вообще приходится дѣлать въ тѣхъ случаяхъ, когда С. С. долженъ выяснить то, что онъ ранѣе не имѣлъ въ виду. Такимъ образомъ, если при производствѣ слѣдствія обнаружилось употребленіе шифрованнаго письма, С. С. обязанъ вновь разсмотрѣть все слѣдствіе *ad hoc*, обращая вниманіе свое на все, что можетъ имѣть значеніе въ этомъ отношеніи. Затѣмъ слѣдуетъ разсмотрѣть всѣ бумаги или документы, отобранные отъ заподозрѣннаго или вообще пріобщенные къ дѣлу. Сдѣлать это послѣднее С. С. долженъ даже и въ томъ случаѣ, если онъ мнитъ себя помнящимъ содержаніе этихъ бумагъ отъ слова до слова. Послѣ того необходимо, самымъ педантичнымъ образомъ осмотрѣть всю одежду обвиняемаго (карманы, швы, обшлага и пр.) и все написанное или печатное, будь то слова, буквы, цифры, знаки, описать и пріобщить къ дѣлу.

Письма же и замѣтки, какія оказались, требуютъ самаго тщательнаго и вдумчиваго осмотра. Изъ содержанія ихъ не только можно уловить и смыслъ шифрованной корреспонденціи, но и даже почерпнуть основанія для разбора шифра. Напр., можетъ быть указанъ способъ чтенія какого-нибудь прежняго шифрованнаго письма, можетъ встрѣтиться неподходящее къ мѣсту слово (напр., посреди фразы), или же одно слово будетъ подчеркнуто, такъ что можно предположить, не есть ли это слово ключъ шифра. Безъ знанія этого слова нѣтъ возможности разгадать шифрованное письмо, и возможно, что обвиняемый для большей вѣрности отмѣтилъ себѣ это слово именно подчеркиваніемъ. Нерѣдко бываетъ, что такой ключъ, будетъ ли имъ слово, цифра, или тайный алфавитъ, написанъ какими-нибудь симпатическими чернилами, напр., чернилами Видемана. Необходимо поэтому осмотрѣть и изслѣдовать всѣ найденные чистые клочки бумаги и въ особенности удостовѣриться въ томъ, не скрыты ли такія отмѣтки между строками исписанной бумаги.

Позволю себѣ разсказать здѣсь одинъ случай о шифрѣ, при-

мѣненномъ въ одномъ гражданскомъ дѣлѣ: случай этотъ долженъ для насъ представлять особый интересъ. По дѣлу о взысканіи съ одного старика-крестьянина за забранный товаръ, этотъ послѣдній въ качествѣ отвѣтчика продставилъ старый календарь, въ которомъ оказались такого рода изображенія (см. ниже рис. 81).

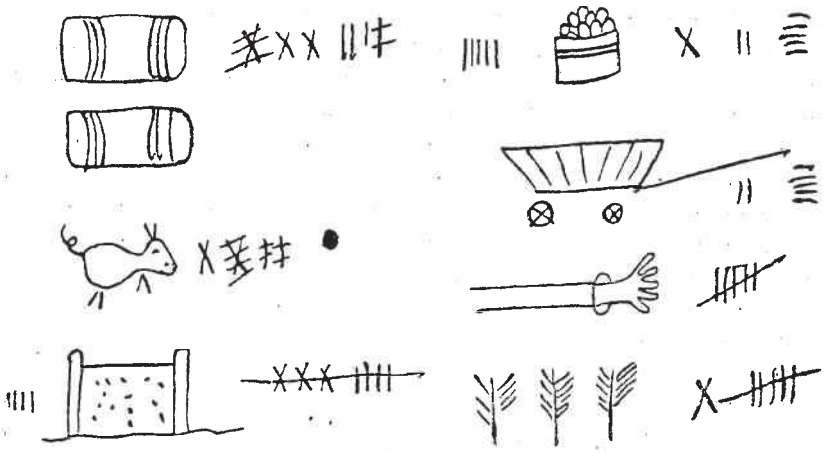

Рис. 81. Мнимый шифръ.

По объясненію крестьянина, такимъ способомъ онъ изобразилъ счетъ долговъ своихъ истцу, такъ какъ онъ не умѣлъ ни читать, ни писать и зналъ только игру въ тарокъ и поэтому также и римскія цифры. Изображенное онъ прочиталъ такъ: 2 бочки вина за 34 гульдена, изъ которыхъ уплочено 11, осталось неуплоченными 23 гул.

1 свинья за 22 гульдена, уплочено 12, осталось 10 гульден.,

4 сажени дровъ за 34 гульдена, уплочено все.

5 мѣръ картофеля за 12 гульденовъ и 50 крейцеровъ, неуплочены, осталось 12 г. 50 крейц.

Одна подвода за 2 гульд. 50 крейц., не уплочено, осталось 2 г. 50 крейц.

Наличными деньгами взято взаймы 5 гульденовъ, уплочены всѣ.

3 бревна за 15 гульд., уплочено 5, осталось 10 гульденовъ.

Предположимъ, что подобный этому шифръ найденъ у тяжкаго преступника; на первый взглядъ покажется невозможнымъ подъискать къ нему ключъ, но если имѣть въ виду, что иногда такіе шифры оказываются весьма просты, то все прочитывается какъ обыкновенное письмо.

И дѣйствительно, совершенно случайныя данныя могутъ иногда помочь дѣлу. Такъ, одинъ обвиняемый, который велъ обширную переписку посредствомъ шифра, имѣлъ при себѣ карманные часы, на внутренней сторонѣ крышки которыхъ былъ фабричный номеръ 27491. При всѣхъ усиліяхъ нельзя было разобрать его рукописей, пока не напали на этотъ номеръ, весьма удобный для автора, такъ какъ онъ, въ случаѣ запамятованія, всегда имѣлъ возможность заглянуть въ часы. И въ самомъ дѣлѣ, съ помощью найденнаго въ часахъ числа, удалось безъ труда прочесть всю корреспонденцію, шифрированную по способу графа Гронфельда (alias генерала Трошю). Возможно также, что обвиняемый постоянно носитъ карманный словарь, который, если только напечатанъ въ два столбца, можетъ свидѣтельствовать о примѣненіи шифра, заключающагося въ замѣнѣ словъ другими словами, и тѣмъ способствовать къ прочтенію писемъ. Наконецъ, возможно, что преступникъ гдѣлибо въ потаенномъ мѣстѣ своей одежды носитъ спрятаннымъ такъ наз. «шаблонъ», съ помощью котораго можно читать шифрованныя его письма; короче говоря, и въ этомъ отношеніи преступникъ часто дѣлаетъ ту «одну большую глупость», которая ведетъ къ его изобличенію. Глупость эта заключается въ томъ, что онъ носитъ при себѣ секретное слово, или цифру, или книгу съ такими знаками, считая этотъ способъ наивѣрнѣйшимъ и не предвидя возможности задержанія его. Говоря коротко, если С. С. все, добытое слѣдствіемъ и почерпнутое изъ шифрованной переписки, сопоставитъ, подвергнетъ разслѣдованіямъ, съумѣетъ комбинировать, то къ нему приходитъ навстрѣчу именно то, что мы называемъ «счастливой случайностью», и въ ней онъ находитъ точки опоры для дальнѣйшихъ дѣйствій и даже, быть можетъ, полное разъясненіе дѣла.

---

2. Различныя системы тайнописи.

Приступая къ перечисленію и описанію наиболѣе употребительныхъ системъ шифра, я долженъ сказать, что мною выбраны лишь системы, которыя вполнѣ доступны личнымъ усиліямъ С. С. или вслѣдствіе ихъ несложности, или потому, что къ нимъ возможно найти ключъ. Но одно обладаніе ключемъ еще ничего не значитъ, если неизвѣстны конструкція шифра и способъ, какъ должно примѣнять ключъ, а въ нѣкоторыхъ случаяхъ и самый

ключъ нельзя найти, разъ не имѣешь понятія о системѣ шифра. Если, напр., у заподозрѣннаго найдены какія-либо отмѣтки въ видѣ цифры, слова, или стиха, или при немъ окажется книга, одно присутствіе которой является подозрительнымъ, то открытіе такого рода можетъ быть полезнымъ только тогда, если извѣстны основанія системы шифра. Всѣ же безспорно трудныя системы шифра, которыя и съ ключемъ невозможно прочесть, мною опущены.

Послѣдующее не есть что-либо новое, а просто представляетъ собой выдержки изъ разныхъ учебниковъ, преимущественно Клюбера, Флейснера ф. Востровичъ, и кое-что я заимствовалъ изъ нѣкоторыхъ журналовъ.

Во *всѣхъ* шифрахъ предполагаются извѣстные условные знаки, имѣющіе общее значеніе: a) non valeurs, «слѣпые знаки», т. е., не имѣющіе никакого значенія и преслѣдующіе цѣль лишь вводить читающаго въ заблужденіе; такъ напр., можетъ быть обусловлено, чтобы переписывающіеся опускали, не считали всѣхъ помѣщенныхъ гласныхъ, или каждую третью букву, или всѣ буквы, число которыхъ по счету дѣлится на шесть и т. д. Не требуется особаго уговора между переписывающимися на т. наз. «шаблонномъ» письмѣ, при которомъ читается лишь то, что видно сквозь вырѣзки шаблона: всѣ же лишніе знаки и безъ того прикрываются невырѣзанными частями шаблона;

b) знаки обратнаго значенія, т. е. такіе, которые показываютъ, что слѣдующую фразу нужно понимать въ обратномъ смыслѣ; напр., «онъ относится къ намъ дружелюбно», т. е. враждебно;

c) знаки уничтожающаго значенія, которые указываютъ, что все сообщенное недѣйствительно и сдѣлано съ цѣлью ввести въ заблужденіе; С. С. приходится особенно считаться съ сообщеніями именно этого рода, такъ какъ они могутъ направить слѣдствіе по совершенно ложному пути;

d) знаки перемѣны, указывающіе, что съ даннаго момента слѣдуетъ читать по иной системѣ, на другомъ языкѣ, справа налѣво и т. п.

Изъ отдѣльныхъ системъ укажемъ слѣдующія:

a) Шифры цифровые.

1. Самое несложное письмо посредствомъ цифръ заключается въ томъ, что каждая буква, часто употребляемыя слова или фразы замѣняются одной или нѣсколькими цифрами; въ послѣднемъ же случаѣ онѣ чередуются.

2. Столь же несложенъ способъ, въ которомъ буквы замѣняются двумя цифрами на основаніи такой комбинаціи: всѣ буквы раздѣляются на группы, которыя затѣмъ и нумеруются, а именно:

cglpty	*aeinrw*	*bfkosx*	*dhmqz*	*uv*
4	3	7	1	8

Каждая буква депеши составляется изъ двухъ цифръ, изъ которыхъ послѣдняя обозначаетъ номеръ группы, а первая—ея мѣсто въ этой группѣ. Напр., слово «Morgen (утро)» пишется шифромъ:

31 47 53 24 23 43

3. Сюда же слѣдуетъ отнести и цифровое письмо, приписываемое Мирабо. Буквы раздѣляются на 5 группъ, каждая изъ которыхъ снабжается номерами, напр.:

1.	2.	3.	4.	5.
m a x o k	*r i n v t*	*h b s e q*	*g f c z u*	*p l y d w*
1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5	1 2 3 4 5

Каждая буква изображается дробью такимъ образомъ, что числителемъ ея будетъ номеръ группы, а знаменателемъ номеръ мѣста буквы въ группѣ и, такъ какъ при этой системѣ не употребляется цифръ свыше 5, то цифры 6—9 и 0 примѣняются, какъ non valeurs, для того, чтобы ввести въ заблужденіе посторонникъ. Такъ напр., можно написать слово «Schweigen (молчать)» такъ:

$$\frac{83}{73}\ \frac{46}{30}\ \frac{39}{16}\ \frac{50}{85}\ \frac{93}{74}\ \frac{28}{92}\ \frac{40}{18}\ \frac{36}{64}\ \frac{29}{37}$$

4. Подвижной (перемѣстительный) цифровой шифръ, примѣнявшійся австрійцами въ Мексикѣ, состоитъ изъ алфавита, передвигающагося между двумя рядами цифръ, въ верхнемъ находятся нечетныя двухцифровыя числа и внизу — четныя двухцифровыя, такъ что каждая буква можетъ обозначаться однимъ четнымъ и однимъ нечетнымъ числами. Чтобы поставить алфавитъ, необходима условная буква: такую букву обозначаетъ первая цифра шифрованной записки; она указываетъ, къ какому ряду чиселъ былъ примѣненъ алфавитъ. Когда алфавитъ перемѣняется, въ качествѣ знака перемѣны употребляется число, расположенное сверху или снизу черты алфавита; слѣдующая за ней цифра является уже условной буквой новаго алфавита.

b) шифры буквенные.

1) Простѣйшій видъ такихъ шифровъ, «шифръ Юлія Цезаря», состоитъ въ томъ, что буквы просто переставляются, напр., взамѣнъ а ставится ф, вмѣсто ж—з и т. д. Насколько неопасенъ по своей незамысловатости этотъ шифръ, настолько же часто онъ употребляется, и навѣрное не одинъ разъ встрѣчался въ практикѣ каждаго С. С. Само собой разумѣется, этотъ видъ шифра можно сдѣлать болѣе сложнымъ, если, напр., писать слова безъ всякихъ промежутковъ или дѣлать промежутки невѣрные, если вставлять еще non valeurs, или примѣняя систему аббата Тритгейма [1]), предложившаго цѣлый рядъ алфавитовъ для употребленія ихъ въ одномъ и томъ же шифрованномъ сообщеніи въ опредѣленномъ порядкѣ. Такъ напр., первая строка (или слово, или фраза) пишется по первому алфавиту, вторая—по слѣдующему и т. д., вслѣдствіе чего прочтеніе такой депеши является значительно затрудненнымъ.

2. Нѣчто подобное представляетъ система буквъ Крона («Buchstaben und Zahlensysteme für die Chiffrierung von Telegrammen, Briefen und Postkarten». Крона. Берлинъ 1893 г.). Система эта во всякомъ случаѣ настолько сложна, что разобраться въ ней С. С. не легко.

3. Довольно часто употребляются шифры изъ гласныхъ, одинъ изъ ключей которыхъ приведенъ ниже: порядокъ гласныхъ, конечно, можно мѣнять, какъ угодно. Каждая буква замѣняется по этому ключу двумя гласными: первою берется крайняя гласная, стоящая влѣво, а слѣдующею—расположенная крайнею вверхъ, такъ напр., *e* = *oe*, *i* = *ie*, *g* = *ao*. Такимъ образомъ слово «abreisen (уѣхать)» будетъ написано—*oioiiieuiiiueae*. Это кажется совершенной безсмыслицей, и ее можно сдѣлать еще запутаннѣе, если въ качествѣ non valeurs ввести согласныя буквы и затѣмъ образовать слова съ произвольными промежутками, напр., то же слово въ такомъ видѣ: *Oki und dom uns in huber und unsinn um und der amme*. Разборъ такого шифра крайне затруднителенъ, такъ какъ всѣ сочетанія буквъ, отдѣленныя промежутками, могутъ быть принимаемы за отдѣльныя слова.

---

[1]) Извѣстный „полигисторъ“ Гейденбергъ, впослѣдствіи I. Тритгеймъ, аббатъ Спонгеймскій и настоятель монастыря св. Іакова близъ г. Вюрцбурга (1462—1516 г.).

4. Дальнѣйшимъ усовершенствованіемъ этихъ шифровъ является шифръ множительный, т. наз. chiffre quarré, chiffre par excellence, chiffre indéchiffrable, изобрѣтеніе котораго приписываютъ дипломату Блэзу де Вижнэръ въ 1859 г. Этотъ видъ шифровъ является самымъ употребительнымъ, такъ какъ онъ въ извѣстной степени гарантированъ отъ разгадыванія, не труденъ для употребленія и не требуетъ, чтобы пользующійся имъ постоянно имѣлъ при себѣ таблицу буквъ (изображеніе ея на слѣдующей страницѣ). Въ случаѣ крайности, такую таблицу можно составить по памяти. Для этого шифра требуются такимъ образомъ таблица буквъ и затѣмъ секретное слово. Положимъ, что такимъ словомъ будетъ «Leipzig» и нужно дать извѣщеніе: «*Einstweilen nichts thun*» (пока ничего не предпринимать). Это извѣщеніе надо раздѣлить по буквамъ и подъ каждой изъ нихъ поставить по буквѣ секретнаго слова въ ихъ послѣдовательности. Когда буквы секретнаго слова исчерпываются, слѣдуетъ снова его начинать, прерывая тамъ, гдѣ слово извѣщенія оканчивается, и продолжая на слѣдующемъ словѣ. Слѣдовательно такъ:

	a	e	i	o	u
u	d	e	r	b	i
o	q	w	a	p	h
i	l	z	k	y	s
e	m	f	v	o	c
a	x	u	u	g	t

Einstweilen nichts tun
LeipzigLeipzigLeipzi

Затѣмъ первая буква текста, слѣдовательно *e*, отыскивается въ первой *горизонтальной* линіи таблицы, и первая буква секретнаго слова (*l*) въ первой *вертикальной* линіи таблицы; отъ первой буквы проводимъ мысленно линію внизъ, а отъ второй буквы *l* вправо, линіи пересѣкутся на буквѣ *p*. Такимъ же образомъ слѣдуетъ поступать и съ слѣдующими буквами текста и секретнаго слова. Извѣщеніе въ шифрованномъ видѣ получается такое:

pnvgseltpn (l)mrisxahget.

Чтеніе такой депеши производится такимъ способомъ, что сначала подъ нею пишется условное слово и первая буква его, *l* отыскивается въ первомъ вертикальномъ столбцѣ и вправо отъ нея отыскивается первая буква депеши, значитъ *p*; поднимаясь отъ этой буквы вверхъ, находимъ въ первой горизонтальной линіи букву *e*. Это есть дѣйствительная буква депеши, первая буква

		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
		a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
2	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
3	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
4	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
5	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
6	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
7	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
8	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
9	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
10	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k
11	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l
12	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m
13	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n
14	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o
15	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p
16	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q
17	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
18	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
19	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t
20	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u
21	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v
22	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w
23	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x
24	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
25	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

текста. Затѣмъ въ лѣвомъ вертикальномъ столбцѣ отыскивается слѣдующая буква секретнаго слова, значитъ *e*, отъ нея вправо вторая буква шифрованной депеши, значитъ *n*, и отъ этой послѣдней перпендикулярно вверхъ до буквы *i* и т. д. Это есть вторая буква дѣйствительнаго текста. Такимъ же способомъ и съ примѣненіемъ той же таблицы можно писать и цифрами. Оставляя то же секретное слово и ту же депешу, мы находимъ, что первая буква условнаго слова *l* соотвѣтствуетъ стоящей рядомъ цифрѣ 11, а первая буква текста *e*—стоящей надъ ней цифрѣ 5 и вмѣсто буквы *p* можно поставить сумму этихъ чиселъ, т. е. 16. Послѣдній способъ съ цифрами примѣняется весьма рѣдко.

При разгадкѣ ключа къ шифрованному письму, С. С., какъ сказано выше, часто помогаетъ «счастливая случайность», и именно въ этой послѣдней системѣ шифра случайность есть главное. При обыскѣ въ бумагахъ переписывающихся, С. С. легко можетъ напасть или на таблицу, или на секретное слово. Нерѣдко можно дѣлать предположенія о такомъ словѣ даже на основаніи общаго поведенія человѣка, его отношеній, знакомства и пр. Большею частью это есть какое-нибудь имя и, если только попытаться примѣнить, какъ секретныя слова, нѣсколько именъ людей, связанныхъ съ личностью обвиняемаго, часто можно напасть на ключъ. То же слѣдуетъ сдѣлать и съ именемъ родного города, родной страны, главной рѣки этой страны или города, или же той страны, гдѣ жилъ въ послѣднее время обвиняемый, затѣмъ съ именами лицъ, только что получившихъ извѣстность, или оказавшихъ важныя услуги его родинѣ или даже его профессіи, или ремеслу (напр., сапожникъ можетъ выбрать ключемъ для шифровъ имя Ганса Закса, литографъ—имя Зенефельдера и т. д.).

Образованный человѣкъ весьма рѣдко выбираетъ ключемъ слово совершенно случайное, а необразованный—почти никогда: прирожденная лѣнь, неповоротливость мысли и любовь къ близкому, знакомому имѣютъ и въ этомъ случаѣ свое вліяніе, и онъ скорѣе остановится на чемъ-нибудь ему близкомъ, нежели чуждомъ, далекомъ отъ его интересовъ. Обширнѣйшее поле для всевозможныхъ комбинацій открывается въ этомъ случаѣ, и при нѣкоторомъ трудѣ успѣхъ не заставитъ себя ждать.

5. На такой же идеѣ основанъ и шифръ Наполеона I-го, изобрѣтенный приблизительно около 1540 г. итальянцемъ Giambatista della Porta. Здѣсь также необходимо секретное слово; таблица же состоитъ изъ особыхъ секретныхъ алфавитовъ на каждыя двѣ

буквы общаго алфавита: первая половина каждаго изъ этихъ секретныхъ алфавитовъ пишется правильно, а вторая половина, располагаемая во второй горизонтальной строкѣ, съ перетасовкой буквъ, изображенной въ нижеприведенной таблицѣ; буквы *k*, *u* и *w* при этомъ исключаются.

A	*B*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*
		n	*o*	*p*	*q*	*r*	*s*	*t*	*v*	*x*	*y*	*z*
C	*D*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*
		z	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*v*	*x*	*y*
E	*F*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*
		y	*z*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*v*	*x*

Возьмемъ въ качествѣ секретнаго слова «*bec*», которое и пишется подъ текстомъ такъ, чтобы каждая буква этого слова приходилась подъ буквой текста. Буква секретнаго слова указываетъ, какой алфавитъ слѣдуетъ примѣнить для замѣны буквы текста.

6. Шифръ гр. Гронфельда (онъ же генералъ Трошю) отличается своей несложностью. Для него требуется только одно условное число, о которомъ должны знать обѣ переписывающіяся стороны, и затѣмъ опредѣленный алфавитъ (слѣдуетъ только условиться, удержаны ли въ немъ буквы *j* и *y*). Положимъ, условнымъ числомъ будетъ 519 и алфавитъ будетъ установленъ такой:

abcdefghiklmnopqrstuvwxyz

Требуется зашифровать «alles gut» (все обстоитъ благополучно). Текстъ пишется съ раздѣленіемъ буквъ одна отъ другой, и подъ каждой изъ нихъ пишется по цифрѣ секретнаго слова столько разъ, сколько придется. Затѣмъ вмѣсто каждой буквы текста пишется та буква алфавита, которая по счету оказывается первою вслѣдъ за такимъ количествомъ буквъ, какое показываетъ цифра, стоящая внизу, при чемъ счетъ производится вправо. Такъ, подъ первой буквой *a* стоитъ цифра 5, поэтому вмѣсто *a* ставится въ шифрованной депешѣ шестая буква алфавита *f*. Подъ второй буквой текста *l* стоитъ цифра 1, поэтому вмѣсто нея ставится вторая буква послѣ *l*, т. е. *m*. Въ шифрованномъ видѣ депеша получаетъ такой видъ:

f m n k t q z u

Прочитать такую депешу невозможно безъ знанія ключа, т. е. условнаго числа. И вотъ тутъ-то легко можетъ случиться, что

этотъ ключъ можетъ быть найденъ у переписывающихся съ извѣстнымъ лицомъ въ видѣ отмѣтки гдѣ-либо. Если имѣется ключъ, то число надо подписать подъ шифрованнымъ текстомъ и въ алфавитѣ отсчитывать влѣво отъ данной буквы шифрованной депеши столько, сколько показываетъ стоящее подъ нею число. Значитъ, вмѣсто *f* будетъ налѣво 5-я буква, т. е. *a*, вмѣсто *m* первая, значитъ *l*, и т. д.

c) шифры изъ слоговъ и цѣлыхъ словъ.

1. Шифры изъ слоговъ заключаются въ томъ, что заранѣе опредѣляется, какіе слоги должны считаться получателемъ письма за дѣйствительно имѣющіе значеніе. Напр., можетъ быть условлено, что въ каждой четной строкѣ письма имѣетъ значеніе первый слогъ третьяго слова. Этотъ видъ шифра весьма надеженъ, если примѣненъ съ надлежащею ловкостью: но для этого требуется особая даровитость, вотъ почему встрѣтить такой шифръ возможно лишь въ видѣ исключенія. Если же письмо прошифровано неудачно, то стиль получается неестественный и невольно навлекаетъ подозрѣніе.

2. Шифры изъ словъ: а) по способу Гейделя. Письмо должно состоять изъ двухъ частей: или собственно письма и приписки, или же въ письмѣ вторая его половина начинается съ новой строки (другихъ «новыхъ» строкъ въ немъ быть не должно). Секретное сообщеніе заключается въ нѣкоторыхъ словахъ первой половины или первой части письма, при чемъ эти слова должны быть размѣщены въ правильномъ ихъ порядкѣ. Вторая же часть письма содержитъ ключъ: на мѣстѣ, по счету соотвѣтствующемъ первому слову секретнаго сообщенія (въ первой части), находится начинающееся съ буквы *D* условное слово. Напр., нужно зашифровать сообщеніе: «*Ich komme morgen zu dir*», т. е. я зайду завтра къ тебѣ. Это письмо можно зашифровать такъ:

«*Ich* theile dir mit, dass ich, wenn ich *komme*, dir alles sagen werde, was *morgen* zu geschehen hat; *zu* meiner Freude kommt auch mein Bruder zu *dir*.

«*Das* schwierigste von allem wird aber gewiss sein, *dass* wir nichts vergessen, was uns *der* Vater sagte, weil *du* stets bedenken musst, was wir von je *dem* Vater schulden».

Въ первой части слѣдуетъ такимъ образомъ читать 1, 9, 15, 19 и 27-е слова, во второй же части всѣ слова, занимающія по

счету такія же мѣста, начинаются съ буквы *D*, почему и можно заключить о томъ, какія именно слова слѣдуетъ читать въ первой половинѣ письма. Этотъ способъ пригоденъ для краткихъ сообщеній, но разоблачить секретъ нетрудно вслѣдствіе неестественнаго, тяжелаго слога.

b) Зашифрованіе при помощи книгъ заключается въ томъ, что оба переписывающіеся имѣютъ одну и ту же книгу одного изданія и условливаются въ томъ, что каждая буква обозначается тремя числами: страницы, строки и буквы. Напр., если нужно замѣнить букву *G*, то она отыскивается въ условленной книгѣ; положимъ, что она окажется на 4-й страницѣ, въ 3-й строкѣ 17-й буквой, такимъ образомъ букву *G* обозначаютъ 4, 3, 17. Такимъ образомъ шифры этого рода невозможно разгадать безъ нахожденія условленной книги. При обыскѣ у заподозрѣннаго лица, С. С. не трудно въ этихъ случаяхъ найти какую нибудь книгу, спрятанную или положенную въ обстановкѣ болѣе или менѣе подозрительной: на всякій случай слѣдуетъ объ этомъ запомнить и, при обнаруженіи шифрованной переписки, попытаться примѣнить ее къ разгадкѣ ключа.

c) Шифръ при помощи словаря примѣняется такимъ образомъ, что переписывающіеся сговариваются о пріобрѣтеніи одного и того же словаря одного изданія, въ два столбца напечатаннаго, и каждое слово секретнаго сообщенія замѣняется словомъ, которое будетъ найдено въ словарѣ на той же страницѣ и строкѣ, но въ сосѣднемъ столбцѣ. Шифрованіе идетъ быстро и легко, но и прочтеніе секретнаго сообщенія производится также безъ затрудненій. Недостатокъ этого шифра заключается въ томъ, что, во избѣжаніе неясностей и недоразумѣній и затѣмъ въ виду возможности легкаго обнаруженія употребленной шифровой системы, приходится избѣгать склоненія и спряженія словъ. Если даже при обыскѣ и не удастся найти такой словарь, то С. С., если онъ имѣетъ свѣдѣнія, что примѣненъ шифръ именно этого рода, можетъ сдѣлать опытъ прочтенія переписки посредствомъ другихъ карманныхъ словарей. Имѣя свѣдѣнія и ознакомившись съ личностями переписывавшихся, С. С. легко можетъ предположить, гдѣ они могли пріобрѣсти себѣ словари. Понятно, что они не могли пользоваться словаремъ, находившимся въ домѣ, быть можетъ, не одинъ десятокъ лѣтъ, такъ какъ нигдѣ такое изданіе не пріобрѣтается въ двухъ экземплярахъ. По всей вѣроятности, оба лексикона они пріобрѣли покупкой спеціально для своей цѣли, и объ этой покупкѣ, быть можетъ, удастся дознать.

d) Къ наиболѣе усовершенствованному виду шифровъ этого рода принадлежитъ шифръ, основаніемъ котораго служитъ особый составленный для этого словарь, въ которомъ каждое слово, каждый письменный знакъ, цифра означается группой цифръ или буквъ. Для сообщенія особой важности, кромѣ того практикуется осложненіе посредствомъ вычитанія или сложенія заранѣе опредѣленнаго секретнаго числа, или иными подобными способами. Однимъ изъ лучшихъ словарей этого рода считается словарь Нитэ (Niethe), заключающій въ себѣ болѣе 20,000 нѣмецкихъ словъ, начинающійся съ числа 5001 и оканчивающійся свыше 31,000. Но и при пользованіи словаремъ помѣщенныя въ немъ цифры не служатъ сами по себѣ, какъ шифры, а употребляются измѣненными посредствомъ сложенія или вычитанія условленнаго числа. Кто пожелаетъ познакомиться съ этимъ дѣломъ ближе, пусть прочтетъ книгу Нитэ «Das bei der Chiffrierabtheilung des deutschen Reichskanzleramts eingeführte telegraphische Chiffriersystem». Во многихъ коммерческихъ кругахъ принятъ шифрованный словарь, выработанный Международнымъ телеграфнымъ бюро въ Бернѣ; въ словарѣ этомъ подлинныя слова замѣняются другими словами изъ болѣе извѣстныхъ культурныхъ языковъ.

d) шифры съ перемѣщеніями при помощи патроновъ и сѣтокъ.

Примѣненіе шифровъ этого рода заключается въ томъ, что какъ при писаніи, такъ и при чтеніи на шифрованное сообщеніе накладывается особая вырѣзка (пробуравленные патроны) или же подкладывается внизъ особая сѣтка. Такъ какъ при этомъ способѣ не всѣ буквы приходятся точно въ строку, то не трудно догадаться о примѣненіи этого шифра. Этотъ способъ имѣетъ безчисленное множество видовъ, имъ пользовались еще криптографы 16-го столѣтія (Кардануст, Ф. Глаубургъ, Тритгеймъ, Порта и др.), но самымъ совершеннымъ и остроумнымъ способомъ слѣдуетъ признать шифры, изобрѣтенные Фламмомъ и Флейснеромъ.

Если С. С. не удастся найти при обыскахъ «шаблона», вырѣзанной накладки (патроновъ) или сѣтки, то онъ не въ состояніи будетъ прочесть шифрованныя этимъ способомъ письма. Но если онъ найдетъ между вещами переписывающихся этотъ ключъ, то весьма скоро разгадаетъ написанное. Не легко однако отыскиваются такіе ключи, такъ какъ они могутъ быть запрятаны въ самыхъ незначительныхъ помѣщеніяхъ, щеляхъ и под.: искать ихъ нужно

ности этого вида шифра. Но если ему извѣстны обычные главные виды шифровъ, то онъ будетъ въ состояніи даже новый, ему еще неизвѣстный, способъ шифрованія подвести подъ одну изъ знакомыхъ ему категорій и отсюда опредѣлить, какъ взяться за дѣло. Затѣмъ знаніе различныхъ системъ шифровъ не только открываетъ ему возможность отнести данный шифръ къ той или другой системѣ, но и помогаетъ ему разрѣшить вопросъ, можетъ ли онъ надѣяться на успѣхъ лично, или же ему слѣдуетъ обратиться къ болѣе свѣдущему лицу.

Полезно соблюдать во всѣхъ случаяхъ пріемы такого рода: тщательно списать копію шифрованнаго письма, или, еще лучше, снять съ него точный снимокъ на оконномъ стеклѣ или посредствомъ прозрачной бумаги. Затѣмъ слѣдуетъ сдѣлать списокъ всѣхъ имѣющихся въ письмѣ знаковъ, сосчитать ихъ и отмѣтить тѣ, которые повторяются черезъ нѣкоторые промежутки. Послѣ того должно отыскать гласныя буквы и именно въ короткихъ, немногосложныхъ словахъ, такъ какъ гласныя буквы болѣе дають указаній, нежели согласныя. каждую найденную букву слѣдуетъ подписать въ шифрованномъ письмѣ подъ соотвѣтствующимъ знакомъ и, при сомнѣніи въ правильности догадки, поставить за ней вопросительный знакъ.

Перечислять всѣ отдѣльные методы не имѣло бы смысла; мы остановимся только на методѣ разбора шифровъ по *характеру* языка (имѣя въ виду только нѣмецкій языкъ) и выберемъ самый несложный шифръ, «шифръ Юлія Цезаря». Прежде всего изложу «спеціальную теорію», предложенную Клюберомъ, тѣмъ болѣе, что лучшей и не имѣется.

1. Характерной особенностью нѣмецкаго языка является число буквъ—25, отсутствіе монограммъ, т. е. словъ, состоящихъ изъ одной лишь буквы, частое повтореніе двойныхъ буквъ, которыя, если онѣ въ началѣ слова, всегда бываютъ гласныя; частое повтореніе двойныхъ согласныхъ въ концѣ слова и частое повтореніе одной и той же буквы въ многосложныхъ словахъ.

2. Напчаще всего повторяется буква *e*: въ словахъ, состоящихъ изъ двухъ буквъ, она чаще всего—первая буква (напр., er, es); въ болѣе же длинныхъ словахъ—по большей части предпослѣдняя буква (напр., Leistungen).

3. Послѣ *e* чаще всего встрѣчается *n*, затѣмъ *i*; *n* во многихъ длинныхъ словахъ бываетъ на концѣ и въ словахъ, состоящихъ изъ 4 буквъ, большею частью бываетъ вдвойнѣ (wenn, denn, dann, kann).

4. Рѣже, чѣмъ другія согласныя, встрѣчаются *g*, *k*, *p*, *r*, *w*, *z* и самыя рѣдкія—*q*, *x*, *y*.

5. Въ большинствѣ триграммъ (т. е. словъ, состоящихъ изъ трехъ буквъ), оканчивающихся на *e*, предпослѣдней буквой бываетъ *i* (die, wie, sie).

6. Почти неразлучными съ *e* бываетъ *n* и *r*, такъ что *r* часто встрѣчается въ срединѣ, а *n* въ концѣ слова.

7. *a* въ биграммахъ (т. е. словахъ, состоящихъ изъ двухъ буквъ) встрѣчается или впереди, или сзади (an, am, da, ja), въ триграммахъ *a* никогда не встрѣчается въ концѣ, а только или въ началѣ слова, или какъ предпослѣдняя буква (ach, als, auf, aus, gar, das, was, Rad).

8. *o* въ двухъ биграммахъ находится сзади (so и wo), а впереди только въ одной (ob). Въ триграммахъ оно никогда не бываетъ послѣдней буквой, а часто въ срединѣ (vor, von), иногда же и первой буквой, напр., oft, Ohr.

9. Гласная *u* въ биграммахъ чаще бываетъ послѣдней, чѣмъ первой, напр., u чаще встрѣчается, чѣмы um. Въ триграммахъ она очень рѣдко бываетъ въ концѣ, а большею частью въ началѣ или въ срединѣ (und, uns, nur, zum). Легче всего ее розыскать въ связкѣ und.

10. *c* рѣдко встрѣчается въ иныхъ сочетаніяхъ, чѣмъ съ *h* и *k*; *ch* легко обнаруживается, если оно часто встрѣчается передъ *en* (machen, lachen, Nachen, Rechen) и если не встрѣчается, какъ самостоятельная буква: кромѣ того, она обращаетъ на себя вниманіе вслѣдствіе частаго употребленія между *c* и *h*, какъ *sch*.

11. *s* часто встрѣчается передъ *ch* и *t*.

12. Послѣ *sch* не бываетъ иныхъ согласныхъ, кромѣ *l*, *m*, *n*, *r*, *w*.

13. Послѣ двухъ одинаковыхъ согласныхъ рѣдко слѣдуютъ другія согласныя, кромѣ *l* и *h*.

14. Изъ словъ, состоящихъ изъ 4 буквъ, бываютъ только два слова, оканчивающіяся на enn, именно: denn и wenn.

15. Большинство словъ изъ 4 буквъ начинаются съ согласной, за которой слѣдуетъ гласная (bald, dein, doch).

16. Изъ биграммъ чаще всего встрѣчается an, затѣмъ по степени употребительности er, es и zu.

17. Въ триграммахъ средней буквой большею частью является гласная.

18. Если послѣ согласной слѣдуетъ другая согласная, то эта послѣдняя большею частью бываетъ *l* или *r* (blass, brechen, fliegen, frieren, glauben, grell и др.).

На Берлинскомъ международномъ конгрессѣ стенографовъ была избрана, между прочимъ, коммиссія для изслѣдованія вопроса о повторяемости буквъ, корней, приставокъ, сложныхъ словъ и звуковъ въ нѣмецкомъ языкѣ. Затѣмъ въ Германскомъ Имперскомъ Указателѣ отъ 2 сентября 1892 г. было опубликовано, что, по изслѣдованіямъ этой коммиссіи, повторяемость гласныхъ въ нѣмецкомъ языкѣ выражается въ такомъ процентномъ отношеніи: *e* 43%, *i* 15%, *a* 12%, *u* 9%, *ei* 6%, *o* 5%, *ä* 1·86%, *au* 1·69%, *ä* 1·54%, *ö* 0·77%, *eu* 0·76%, *ai* 0·27%, *äu* 0·04%.

Добавлю къ этому нѣсколько обобщеній, заимствованныхъ у Флейснера. 1) Среди сотни буквъ нижеслѣдующія встрѣчаются въ такомъ отношеніи:

e = 18·66	*u* = 5·00	*l* = 2·91	*w* = 1·45
n = 11·33	*d* = 4·83	*b* = 2·67	*k* = 1·21
i = 7·88	*a* = 4·79	*m* = 2·58	*v* = 1·08
r = 7·25	*h* = 4·34	*f* = 1·67	*p* = 0·33
s = 6·75	*g* = 3·96	*z* = 1·62	*j* = 0·12
t = 5·04	*o* = 3·25	*c* = 1·58	

Въ болѣе крупныхъ рукописяхъ приведенныя процентныя отношенія всегда окажутся постоянными.

2. Также и по вопросу, какъ часто встрѣчаются однѣ буквы вмѣстѣ съ другими, можно дать болѣе или менѣе твердыя данныя объ ихъ повторяемости. Въ убывающемъ порядкѣ можно расположить эти буквы такъ: en, er, ch, de, ge, ei, ie, in, ne, be, el, te, st, di, nd, ue, se, au, re, he, при чемъ en встрѣчается въ 18 разъ, чаще he, er въ 13, ch въ 10, de въ 8 разъ чаще, чѣмъ he.

3. По отношенію къ отдѣльнымъ буквамъ Флейснеръ говоритъ такъ: *a* въ триграммахъ никогда не бываетъ въ концѣ слова (исключая иностранныхъ словъ), двойное *b* только въ срединѣ слова (Abbé, Ebbe), ch въ концѣ слова (какъ предпослѣдняя или третья буква съ конца) почти всегда имѣетъ за собой *e* или *t* (Wache, breche, Pracht, Nachricht), *d* встрѣчается во всѣхъ болѣе употребительныхъ триграммахъ (den, der, die, des, das, dem, dir, dis); въ биграммахъ только въ da и du; *g* легче всего обнаруживается въ окончаніи ung, Hoffnung, Labung, Rettung; *h* часто бываетъ между двумя *e* (wehen, gehen), и послѣ *t* (Thal, Wuth) и послѣ *c*, какъ

ch; *l* часто бываетъ вмѣстѣ съ *g* (Glut, gleich, Glaube, folgt, Alge); если послѣ *l* стоитъ другая согласная кромѣ *g*, то ему предшествуетъ гласная (also, selbst); *o*, сравнительно съ другими гласными, встрѣчается рѣже другихъ, сравнительно же вообще съ буквами встрѣчается часто; *r* часто связывается съ *e* [1]).

Если твердо помнить всѣ эти обобщенія, то не трудно прочесть какой-нибудь несложный шифръ.

Въ этомъ отношеніи слѣдуетъ обращать главное вниманіе на все то, что обвиняемый незамѣтно для другихъ пытался отбросить или уничтожить. Вслѣдствіе этого необходимо внушать всѣмъ чинамъ полиціи, производящимъ розыски, чтобы они отнюдь не считали несущественными для дѣла, напр., брошенные клочки бумаги и пр. Можно высказать, какъ общее правило, что задержанный, имѣющій при себѣ шифрованныя письма и ключъ къ нимъ, по задержаніи всегда будетъ стараться ихъ уничтожить, незамѣтно для другихъ присутствующихъ. Если даже полицейскій чиновникъ и замѣтитъ это, то арестованному нетрудно убѣдить его, что брошенная вещь не имѣетъ «никакого значенія», если только жандармъ не имѣетъ представленія и вообще не знаетъ, какое значеніе можетъ имѣть оброненный предметъ. А между тѣмъ клочекъ газетной бумаги, или нитка, или какая-то вырѣзка изъ бумаги, повидимому, совершенно безразличная, можетъ дать исходную точку для слѣдствія и раскрыть дѣло.

---

[1]) Здѣсь мы опускаемъ таблицу, въ которой авторъ приводитъ цифровыя данныя, какіе слоги наиболѣе часто употребляются въ нѣмецкомъ языкѣ и т. п. Примѣч. переводч.