**Лекция 1. Открытые сообщения и их характеристики. Частотные характеристики открытых сообщений. Критерии на открытый текст. Анализ и способы вскрытие простых замен, шифра цезаря и вертикальной перестановки.**

* 1. История развития криптографии
	2. Частотные характеристики открытых сообщений
	3. Простые шифры

История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования. **Первый период** *(приблизительно с 3-го тысячелетия до н. э.)* характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами). **Второй период** *(с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) — до начала XX века)* ознаменовался введением в обиход полиалфавитных шифров. **Третий период** *(с начала и до середины XX века)* характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров. **Четвёртый период** *(с середины до 70-х годов XX века)* период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам — линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической», или же, более корректно, криптографией с секретным ключом.

**Современный период развития криптографии** *(с конца 1970-х годов по настоящее время)* отличается зарождением и развитием нового направления — криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами (в предыдущие эпохи использование криптографии было исключительной прерогативой государства). Правовое регулирование использования криптографии частными лицами в разных странах сильно различается — от разрешения до полного запрета.

**Современная криптография** образует отдельное научное направление на стыке математики и информатики — работы в этой области публикуются в научных журналах, организуются регулярные конференции. Практическое применение криптографии стало неотъемлемой частью жизни современного общества — её используют в таких отраслях как электронная коммерция, электронный документооборот (включая цифровые подписи), телекоммуникации и других.

|  |
| --- |
| **Криптоанализ** (от [др.-греч.](https://ru.wikipedia.org/wiki/%D0%94%D1%80%D0%B5%D0%B2%D0%BD%D0%B5%D0%B3%D1%80%D0%B5%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) κρυπτός — скрытый и [анализ](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7)) — наука о методах расшифровки зашифрованной информации без предназначенного для такой расшифровки [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29).Термин был введён американским криптографом [Уильямом Ф. Фридманом](https://ru.wikipedia.org/wiki/%D0%A4%D1%80%D0%B8%D0%B4%D0%BC%D0%B0%D0%BD%2C_%D0%A3%D0%B8%D0%BB%D1%8C%D1%8F%D0%BC_%D0%A4%D1%80%D0%B5%D0%B4%D0%B5%D1%80%D0%B8%D0%BA) в [1920 году](https://ru.wikipedia.org/wiki/1920_%D0%B3%D0%BE%D0%B4) в рамках его книги «Элементы криптоанализа». Неформально криптоанализ называют также взломом [шифра](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80).В большинстве случаев под криптоанализом понимается выяснение [ключа](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_%28%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%29); криптоанализ включает также методы выявления уязвимости криптографических алгоритмов или протоколов. **Частотный анализ**, **частотный криптоанализ** — один из методов [криптоанализа](http://dic.academic.ru/dic.nsf/ruwiki/80517), основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования. Упрощённо, частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае моноалфавитного шифрования если в [шифротексте](http://dic.academic.ru/dic.nsf/ruwiki/1412251) будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой. Аналогичные рассуждения применяются к биграммам (двубуквенным последовательностям), триграммам и т.д. в случае [полиалфавитных шифров](http://dic.academic.ru/dic.nsf/ruwiki/672132). Начиная с середины XX века большинство используемых алгоритмов шифрования разрабатываются устойчивыми к частотному криптоанализу, поэтому он применяется, в основном, для обучения.В каждом языке разная частота распределения отдельных символов и их сочетаний. Эту особенность языков используют в криптоанализе. В английском языке распределения следущие. http://hellosherlock.narod.ru/theory/dictionary/f/freqleten.gif |
|  |
|  |

В русском языке распределения следущие.

о — 9.28%
а — 8.66%
е — 8.10%
и — 7.45%
н — 6.35%
т — 6.30%
р — 5.53%
с — 5.45%
л — 4.32%
в — 4.19%
к — 3.47%
п — 3.35%
м — 3.29%
у — 2.90%
д — 2.56%
я — 2.22%
ы — 2.11%
ь — 1.90%
з — 1.81%
б — 1.51%
г — 1.41%
й — 1.31%
ч — 1.27%
ю — 1.03%
х — 0.92%
ж — 0.78%
ш — 0.77%
ц — 0.52%
щ — 0.49%
ф — 0.40%
э — 0.17%
ъ — 0.04%

**Шифры простой замены.** При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки.

Также можно зашифровывать сообщения с помощью ЦИФРОВОЙ ТАБЛИЦЫ. Её параметры могут быть какими угодно, главное, чтобы получатель и отправитель были в курсе. Пример цифровой таблицы.



**КНИЖНЫЙ ШИФР.** В таком шифре ключом является некая книга, имеющаяся и у отправителя и у получателя. В шифре обозначается страница книги и строка, первое слово которой и является разгадкой. Дешифровка невозможна, если книги у отправителя и корреспондента разных годов издания и выпуска. Книги обязательно должны быть идентичными.

**ШИФР ЦЕЗАРЯ** (шифр сдвига, сдвиг Цезаря). Известный шифр. Сутью данного шифра является замена одной буквы другой, находящейся на некоторое постоянное число позиций левее или правее от неё в алфавите. Гай Юлий Цезарь использовал этот способ шифрования при переписке со своими генералами для защиты военных сообщений. Этот шифр довольно легко взламывается, поэтому используется редко. Сдвиг на 4. A = E, B= F, C=G, D=H и т.д.
Пример шифра Цезаря: зашифруем слово « DEDUCTION » .Получаем: GHGXFWLRQ

**Дешифрование**

В общем случае при одноалфавитной подстановке происходит однозначная замена исходных символов их эквивалентами из вектора замен (или таблицы замен). При таком методе шифрования ключом является используемая таблица замен.

Подстановка может быть задана с помощью таблицы, например,



В таблице на самом деле объединены сразу две таблицы. Одна (шифр 1) определяет замену русских букв исходного текста на другие русские буквы, а вторая (шифр 2) – замену букв на специальные символы. Исходным алфавитом для обоих шифров будут заглавные русские буквы (за исключением букв "Ё" и "Й"), пробел и точка.

Зашифрованное сообщение с использованием любого шифра моноалфавитной подстановки получается следующим образом. Берется очередной знак из исходного сообщения. Определяется его позиция в столбце "Откр. текст" таблицы замен. В зашифрованное сообщение вставляется шифрованный символ из этой же строки таблицы замен.

Попробуем зашифровать сообщение "ВЫШЛИТЕ ПОДКРЕПЛЕНИЕ" c использованием этих двух шифров. Для этого берем первую букву исходного сообщения "В". В таблице в столбце "Шифр 1" находим для буквы "В" заменяемый символ. Это будет буква "О". Записываем букву "О" под буквой "В". Затем рассматриваем второй символ исходного сообщения – букву "Ы". Находим эту букву в столбце "Откр. текст" и из столбца "Шифр 1" берем букву, стоящую на той же строке, что и буква "Ы". Таким образом получаем второй символ зашифрованного сообщения – букву "Н". Продолжая действовать аналогично, зашифровываем все исходное сообщение.



Полученный таким образом текст имеет сравнительно низкий уровень защиты, так как исходный и зашифрованный тексты имеют одинаковые статистические закономерности. При этом не имеет значения, какие символы использованы для замены – перемешанные символы исходного алфавита или таинственно выглядящие знаки.

Зашифрованное сообщение может быть вскрыто путем так называемого *частотного криптоанализа*. Для этого могут быть использованы некоторые статистические данные языка, на котором написано сообщение.

Известно, что в текстах на русском языке наиболее часто встречаются символы О, И. Немного реже встречаются буквы Е, А. Из согласных самые частые символы Т, Н, Р, С. В распоряжении криптоаналитиков имеются специальные таблицы частот встречаемости символов для текстов разных типов – научных, художественных и т.д.

Криптоаналитик внимательно изучает полученную криптограмму, подсчитывая при этом, какие символы сколько раз встретились. Вначале наиболее часто встречаемые знаки зашифрованного сообщения заменяются, например, буквами О. Далее производится попытка определить места для букв И, Е, А. Затем подставляются наиболее часто встречаемые согласные. На каждом этапе оценивается возможность "сочетания" тех или иных букв. Например, в русских словах трудно найти четыре подряд гласные буквы, слова в русском языке не начинаются с буквы Ы и т.д. На самом деле для каждого естественного языка (русского, английского и т.д.) существует множество закономерностей, которые помогают раскрыть специалисту зашифрованные противником сообщения.

Возможность однозначного криптоанализа напрямую зависит от длины перехваченного сообщения. Посмотрим, с чем это связано. Пусть, например, в руки криптоаналитиков попало зашифрованное с помощью некоторого шифра одноалфавитной замены сообщение:

ТНФЖ.ИПЩЪРЪ

Это сообщение состоит из 11 символов. Пусть известно, что эти символы составляют целое сообщение, а не фрагмент более крупного текста. В этом случае наше зашифрованное сообщение состоит из одного или нескольких целых слов. В зашифрованном сообщении символ Ъ встречается 2 раза. Предположим, что в открытом тексте на месте зашифрованного знака Ъ стоит гласная О, А, И или Е. Подставим на место Ъ эти буквы и оценим возможность дальнейшего криптоанализа [таблица 1](http://www.intuit.ru/studies/courses/691/547/lecture/12373?page=2#table.2.1)

|  |
| --- |
| Таблица 1. Варианты первого этапа криптоанализа |
| Зашифрованное сообщение |
| Т | Н | Ф | Ж | . | И | П | Щ | Ъ | Р | Ъ |
| После замены Ъ на О |
|  |  |  |  |  |  |  |  | О |  | О |
| После замены Ъ на А |
|  |  |  |  |  |  |  |  | А |  | А |
| После замены Ъ на И |
|  |  |  |  |  |  |  |  | И |  | И |
| После замены Ъ на Е |
|  |  |  |  |  |  |  |  | Е |  | Е |

Все приведенные варианты замены могут встретиться на практике. Попробуем подобрать какие-нибудь варианты сообщений, учитывая, что в криптограмме остальные символы встречаются по одному разу.

|  |
| --- |
| Таблица 2. Варианты второго этапа криптоанализа |
| Зашифрованное сообщение |
| Т | Н | Ф | Ж | . | И | П | Щ | Ъ | Р | Ъ |
| Варианты подобранных дешифрованных сообщений |
| Ж | Д | И |  | С | У | М | Р | А | К | А |
| Д | Ж | О | Н | А |  | У | Б | И | Л | И |
| В | С | Е | Х |  | П | О | Б | И | Л | И |
| М | Ы |  | П | О | Б | Е | Д | И | Л | И |

Кроме представленных на [таблица 2](http://www.intuit.ru/studies/courses/691/547/lecture/12373?page=2#table.2.2) сообщений можно подобрать еще большое количество подходящих фраз. Таким образом, если нам ничего не известно заранее о содержании перехваченного сообщения малой длины, дешифровать его однозначно не получится.

Если же в руки криптоаналитиков попадает достаточно длинное сообщение, зашифрованное методом простой замены, его обычно удается успешно дешифровать. На помощь специалистам по вскрытию криптограмм приходят статистические закономерности языка. Чем длиннее зашифрованное сообщение, тем больше вероятность его однозначного дешифрования.

**Пример2.**

Ключ:

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ.\_,-

ЮДТВЕЗИЛМ.НОПСАУФХЦЧКШЖЩЪЙРЫЬЭБЯГ\_,-

Шифрованный текст:

НЮЛЮШХЦЮСВАХЧЕЮФХЦТАФЮХУАОАИЗССАЗТЖЗСЦФЗЗТФЮЛМММСЮХЗВАЕСЯЪСМ.ЕЗСЬУАХТАЗ.УОАЙЮЕМТШАЕЯЙЗЗТЕЗХЯЦНЧНФЧУСЗ.ЪМШХЦФЮСПМФЮГАХАДЗССАХЦЬБЭЦА.ХЦФЮСЫЯТОЯЗЦХЯЦАЩЦААСЮФЮХУАОАИЗСЮТЩЗЦЫФШНОМПЮЦМЩЗХНМШЛАСЮШГУАЭЦАПЧЛЕЗХЬУФЗНФЮХСАХАЩЗЦЮБЦХЯЛЗОЗСЫЗОЧВЮМЛСА.СЫЗУЧХЦЫСМЛЮХСЗИЗССЫЗВАФСЫЗТЗФЪМСЫМСЗУФАШАЕМПЫЗОЗХЮГЭЦАУАЛТАОЯЗЦНЮИЕАПЧЦЧФМХЦЧХЕЗОЮЦЬЕОЯХЗДЯАЦЕЫШТНЮЛЮШХЦЮСЗПЮНХМПЮОЬСАМСЦЗФЗХСЫПМСЮХЫЙЗССЫПГЦЮНСЮУФМПЗФЕОЯОБДМЦЗОЗ.ЮНЦМТСАВААЦЕЫШЮЛЕЗХЬФЮЛПЗЙЗСАПСАИЗХЦТАВАФСЫШЦФАУОЫИСЫШЦФЮХХМПСАИЗХЦТАУЗЙЗФНЮИЕЮЯМЛНАЦАФЫШСЮУФАЦЯИЗСММПСАВМШТЗНАТШФЮСМЦХТАМЦЮ.СЫГ

Открытый текст:

КазахстангосударстворасположенноевцентреЕвразииинасегодняшнийденьпосвоейплощадивходящеевдесяткукрупнейшихстранмира.Особенностьюэтойстраныявляетсяточтоонарасположенавчетырхклиматическихзонах.ПоэтомуздесьпрекрасносочетаютсязелЕныелугаизнойныепустынизаснеженныегорныевершиныинепроходимыелеса.ЭтопозволяеткаждомутуристусделатьдлясебяотдыхвКазахстанемаксимальноинтересныминасыщенным.Такнапримердлялюбителейактивногоотдыхаздесьразмещеномножествогорныхтроплыжныхтрассимножествопещеркаждаяизкоторыхнапротяжениимногихвековхранитсвоитайны.

**Вертикальная перестановка.**

В шифре реализуется перестановка считываемых столбцов матрицы в соответствии с ключом.

**Шифрование:**

Пусть, например, этот ключ таков: (5,4,1,7,2,6,3), и с его помощью надо зашифровать сообщение:

ВОТПРИМЕРШИФРАВЕРТИКАЛЬНОЙПЕРЕСТАНОВКИ

Впишем сообщение в прямоугольник, столбцы которого пронумерованы в соответствии с ключом:

Таблица 1.1

|  |
| --- |
|  |
| 5 | 1 | 4 | 7 | 2 | 6 | 3 |  |
| В | О | Т | П | Р | И | М |  |
| Е | Р | Ш | И | Ф | Р | А |  |
| В | Е | Р | Т | И | К | А |  |
| Л | Ь | Н | О | Й | П | Е |  |
| Р | Е | С | Т | А | Н | О |  |
| В | К | И | - | - | - | - |  |
|  |  |  |  |  |  |  |  |

Теперь, выбирая столбцы в порядке, заданном ключом, и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

ОРЕЬЕКРФИЙА-МААЕО-ТШРНСИВЕВЛРВИРКПН-ПИТОТ-

**Криптоанализ вертикальной перестановки**

В процессе шифрования вертикальными перестановками буквы каждого столбца заполненного прямоугольника выписываются в криптограмму подряд, то есть криптограмма разбивается на отрезки, являющиеся столбцами таблицы. Поэтому при дешифровании естественно попытаться соединить две группы последовательных букв криптограммы так, чтобы они образовывали хорошие с точки зрения обычного текста комбинации.

Для этого естественно использовать наиболее частые биграммы открытого текста, которые можно составить из букв рассматриваемого шифрованного текста.

Если для первой пробы выбрано, скажем, сочетание *СТ* (самая частая биграмма русского языка), то можем по очереди приписывать к каждой букве *С* криптограммы каждую букву *Т* из нее. При этом несколько букв, стоящих до и после данной буквы С, и несколько букв, стоящих до и после данной буквы Т, соединяются в пары, то есть получаются два столбца букв, записанные рядом.

Конечно, длины столбцов не известны, но некоторые ограничения на них можно получить, используя положение конкретных букв. Так, столбцы должны иметь одинаковые длины или первый столбец может быть длиннее второго на одну букву, и тогда эта буква - последняя буква сообщения.

Если приписываемые друг к другу буквы разделены, скажем, только двумя буквами, то, как легко видеть, мы можем составить в соседних столбцах не более трех пар, и длина столбца не превышает четырех. Кроме того, ограничением может послужить появление запретной биграммы (например, гласная - мягкий знак).

Для выбранного сочетания СТ получается по одной паре столбцов для каждого конкретного выбора букв С и Т из криптограммы, и из них целесообразно отобрать ту пару, которая содержит наиболее частые биграммы.

При автоматизации этого процесса можно приписать каждой биграмме вес, равный частоте ее появления в открытом тексте. Тогда следует отобрать ту пару столбцов, которая имеет наибольший вес. Кстати, появление одной биграммы с низкой частотой может указать на то, что длину столбца надо ограничить по длине. Выбран пару столбцов, мы аналогичным образом можем подобрать к ним третий (справа или слева) и т.д.

Описанная процедура значительно упрощается при использовании вероятных слов, то есть слов, которые могут встретиться в тексте с большой вероятностью.



о — 9.28%
а — 8.66%
е — 8.10%
и — 7.45%
н — 6.35%
т — 6.30%
р — 5.53%
с — 5.45%
л — 4.32%
в — 4.19%
к — 3.47%
п — 3.35%
м — 3.29%
у — 2.90%
д — 2.56%
я — 2.22%
ы — 2.11%
ь — 1.90%
з — 1.81%
б — 1.51%
г — 1.41%
й — 1.31%
ч — 1.27%
ю — 1.03%
х — 0.92%
ж — 0.78%
ш — 0.77%
ц — 0.52%
щ — 0.49%
ф — 0.40%
э — 0.17%
ъ — 0.04%

Приведем таблицы частот биграмм для русского и английского языков (таблицы заимствованы из книги [[4]](http://statistica.ru/local-portals/data-mining/analiz-tekstov/#s4)). Для удобства они разбиты на четыре части по следующей схеме:

|  |
| --- |
| **Часть 1** |
|   | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| **А** | 2 | 12 | 35 | 8 | 14 | 7 | 6 | 15 | 7 | 7 | 19 | 27 | 19 | 45 | 5 | 11 |
| **Б** | 5 |   |   |   |   | 9 | 1 |   | 6 |   |   | 6 |   | 2 | 21 |   |
| **В** | 35 | 1 | 5 | 3 | 3 | 32 |   | 2 | 17 |   | 7 | 10 | 3 | 9 | 58 | 6 |
| **Г** | 7 |   |   |   | 3 | 3 |   |   | 5 |   | 1 | 5 |   | 1 | 50 |   |
| **Д** | 25 |   | 3 | 1 | 1 | 29 | 1 | 1 | 13 |   | 1 | 5 | 1 | 13 | 22 | 3 |
| **Е** | 2 | 9 | 18 | 11 | 27 | 7 | 5 | 10 | 6 | 15 | 13 | 35 | 24 | 63 | 7 | 16 |
| **Ж** | 5 | 1 |   |   | 6 | 12 |   |   | 5 |   |   |   |   | 6 |   |   |
| **З** | 35 | 1 | 7 | 1 | 5 | 3 |   |   | 4 |   | 2 | 1 | 2 | 9 | 9 | 1 |
| **И** | 4 | 6 | 22 | 5 | 10 | 21 | 2 | 23 | 19 | 11 | 19 | 21 | 20 | 32 | 8 | 13 |
| **Й** | 1 | 1 | 4 | 1 | 3 |   | 1 | 2 | 4 |   | 5 | 1 | 2 | 7 | 9 | 7 |
| **К** | 24 | 1 | 4 | 1 |   | 4 | 1 | 1 | 26 |   | 1 | 4 | 1 | 2 | 66 | 2 |
| **Л** | 25 | 1 | 1 | 1 | 1 | 33 | 2 | 1 | 36 |   | 1 | 2 | 1 | 8 | 30 | 2 |
| **М** | 18 | 2 | 4 | 1 | 1 | 21 | 1 | 2 | 23 |   | 3 | 1 | 3 | 7 | 19 | 5 |
| **Н** | 54 | 1 | 2 | 3 | 3 | 34 |   |   | 58 |   | 3 |   | 1 | 24 | 67 | 2 |
| **О** | 1 | 28 | 84 | 32 | 47 | 15 | 7 | 18 | 12 | 29 | 19 | 41 | 38 | 30 | 9 | 18 |
| **П** | 7 |   |   |   |   | 15 |   |   | 4 |   |   | 9 |   | 1 | 46 |   |

|  |
| --- |
| **Часть 2** |
|   | **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **А** | 26 | 31 | 27 | 3 | 1 | 10 | 6 | 7 | 10 | 1 |   |   | 2 | 6 | 9 |
| **Б** | 8 | 1 |   | 6 |   |   |   |   |   | 1 | 11 |   |   |   | 2 |
| **В** | 6 | 19 | 6 | 7 |   | 1 | 1 | 2 | 4 | 1 | 18 | 1 | 2 |   | 3 |
| **Г** | 7 |   |   | 2 |   |   |   |   |   |   |   |   |   |   |   |
| **Д** | 6 | 8 | 1 | 10 |   |   | 1 | 1 | 1 |   | 5 | 1 |   |   | 1 |
| **Е** | 39 | 37 | 33 | 3 | 1 | 8 | 3 | 7 | 3 | 3 |   |   | 1 | 1 | 2 |
| **Ж** |   | 1 |   |   |   |   |   |   |   |   |   |   |   |   |   |
| **З** | 3 | 1 |   | 2 |   |   |   |   |   |   | 4 |   |   |   | 4 |
| **И** | 11 | 29 | 29 | 3 | 1 | 17 | 3 | 11 | 1 | 1 |   |   | 1 | 3 | 17 |
| **Й** | 3 | 10 | 2 |   |   |   | 1 | 3 | 2 |   |   |   |   |   |   |
| **К** | 10 | 3 | 7 | 10 |   |   | 1 |   |   |   |   |   |   |   |   |
| **Л** |   | 3 | 1 | 6 |   | 4 |   | 1 |   |   | 3 | 20 |   | 4 | 9 |
| **М** | 2 | 5 | 3 | 9 | 1 |   |   | 2 |   |   | 5 | 1 | 1 |   | 3 |
| **Н** | 1 | 9 | 9 | 7 | 1 |   | 5 | 2 |   |   | 36 | 3 |   |   | 5 |
| **О** | 43 | 50 | 39 | 3 | 2 | 5 | 2 | 12 | 4 | 3 |   |   | 2 | 3 | 2 |
| **П** | 41 | 1 |   | 6 |   |   |   |   |   |   | 2 |   |   |   | 2 |

|  |
| --- |
| **Часть 3** |
|   | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| **Р** | 55 | 1 | 4 | 4 | 3 | 37 | 3 | 1 | 24 |   | 3 | 1 | 3 | 7 | 56 | 2 |
| **С** | 8 | 1 | 7 | 1 | 2 | 25 |   |   | 6 |   | 40 | 13 | 3 | 9 | 27 | 11 |
| **Т** | 35 | 1 | 27 | 1 | 3 | 31 |   | 1 | 28 |   | 5 | 1 | 1 | 11 | 56 | 4 |
| **У** | 1 | 4 | 4 | 4 | 11 | 2 | 6 | 3 | 2 |   | 8 | 5 | 5 | 5 | 1 | 5 |
| **Ф** | 2 |   |   |   |   | 2 |   |   | 2 |   |   |   |   |   | 1 |   |
| **Х** | 4 | 1 | 4 | 1 | 3 | 1 |   | 2 | 3 |   | 4 | 3 | 3 | 4 | 18 | 5 |
| **Ц** | 3 |   |   |   |   | 7 |   |   | 10 |   | 2 |   |   |   | 1 |   |
| **Ч** | 12 |   |   |   |   | 23 |   |   | 13 |   | 2 |   |   | 6 |   |   |
| **Ш** | 5 |   |   |   |   | 11 |   |   | 14 |   | 1 | 2 |   | 2 | 2 |   |
| **Щ** | 3 |   |   |   |   | 8 |   |   | 6 |   |   |   |   | 1 |   |   |
| **Ы** |   | 1 | 9 | 1 | 3 | 12 |   | 2 | 4 | 7 | 3 | 6 | 6 | 3 | 2 | 10 |
| **Ь** |   | 2 | 4 | 1 | 1 | 2 |   | 2 | 2 |   | 6 |   | 3 | 13 | 2 | 4 |
| **Э** |   |   |   |   |   |   |   |   |   |   | 1 |   |   | 1 |   |   |
| **Ю** |   | 2 | 1 | 2 | 1 |   |   | 3 | 1 |   | 1 |   | 1 | 1 | 1 | 3 |
| **Я** | 1 | 3 | 9 | 1 | 3 | 3 | 1 | 5 | 3 | 2 | 3 | 3 | 4 | 6 | 3 | 6 |

|  |
| --- |
| **Часть 4** |
|   | **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **Р** | 1 | 5 | 9 | 16 |   | 1 | 1 | 1 | 2 |   | 8 | 3 |   |   | 5 |
| **С** | 4 | 11 | 82 | 6 |   | 1 | 1 | 2 | 2 |   | 1 | 8 |   |   | 17 |
| **Т** | 26 | 18 | 2 | 10 |   |   |   | 1 |   |   | 11 | 21 |   |   | 4 |
| **У** | 7 | 14 | 7 |   |   | 1 |   | 8 | 3 | 2 |   |   |   | 9 | 1 |
| **Ф** | 1 | 1 |   |   |   |   |   |   |   |   |   |   |   |   |   |
| **Х** | 3 | 4 | 2 | 2 | 1 |   |   | 1 |   |   |   |   |   |   |   |
| **Ц** |   |   |   | 1 |   |   |   |   |   |   | 1 |   |   |   |   |
| **Ч** |   |   | 7 | 1 |   |   |   |   | 1 |   |   | 1 |   |   |   |
| **Ш** |   |   |   | 1 |   |   |   |   |   |   |   | 1 |   |   |   |
| **Щ** |   |   |   | 1 |   |   |   |   |   |   |   |   |   |   |   |
| **Ы** | 3 | 9 | 4 | 1 |   | 16 |   | 1 | 2 |   |   |   |   |   |   |
| **Ь** | 1 | 11 | 3 |   |   |   |   | 1 | 4 |   |   |   | 1 | 3 | 1 |
| **Э** |   | 1 | 9 |   |   |   |   |   |   |   |   |   |   |   |   |
| **Ю** | 1 | 1 | 7 |   |   |   | 1 | 1 |   | 4 |   |   |   |   |   |
| **Я** | 3 | 6 | 10 |   |   | 2 | 1 | 4 | 1 | 1 |   |   | 1 | 1 | 1 |

 **СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО
СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА**

Такого рода шифры легко ломаются. Дело в том, что они никак не путают статистику символов открытого текста.