Южный федеральный университет

Факультет математики, механики и компьютерных наук

В.С. Пилиди

Электронное учебное пособие

Криптография. Вводные главы

Ростов-на-Дону
2009

Управляющие клавиши

Результат	**Действие**
Включить/выключить оглавление	**F4**
Вся страница	**Ctrl+L**
Предыдущий экран	**PgUp**
Следующий экран	**PgDn**
Первая страница	**Home**
Последняя страница	**End**
Следующая страница	→
Предыдущая страница	←
Следующий вид	**Alt +** →
Предыдущий вид	**Alt +** ←
Увеличить Уменьшить	**Ctrl + «знак равенства»** **Ctrl + «дефис»**

Глава 1. Некоторые простые криптосистемы.

Основная цель криптографии состоит в том, чтобы позволить двум лицам связаться по ненадежному каналу так, чтобы противник не мог понять смысла передаваемой информации. Этот канал может быть, например, телефонной линией или компьютерной сетью. Информация, которую отправитель хочет послать получателю, обычно называется *открытым текстом* и может быть в буквальном смысле текстом на каком-либо языке, числовыми данными, или чем-либо иным. Предполагается, что структура открытого текста полностью произвольна. Отправитель *шифрует* открытый текст, используя заранее выбранный *ключ*, и посылает получаемый *шифртекст* по используемому каналу. Противник (или нарушитель), перехватив шифртекст, не может восстановить исходный открытый текст, но получатель, знающий ключ шифрования, может провести дешифрование и восстановить исходный открытый текст.

Формализация приведенного процесса дается следующим определением.

ОПРЕДЕЛЕНИЕ. *Криптосистемой называется набор из пяти непустых конечных множеств* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$*, называемых, как указано ниже, и обладающих следующими свойствами:*

1. $\mathcal{P}$*,* $\mathcal{C}$ *и* $\mathcal{K}$ *называются соответственно множеством символов открытого текста, множеством символов шифртекста и множеством ключей;*

2. $\mathcal{E}$ *— множество отображений множества* $\mathcal{P}$ *в множество* $\mathcal{C}$*,*

называемых отображениями шифрования;

3. $\mathcal{D}$ *— множество отображений множества* $\mathcal{C}$ *в множество* $\mathcal{P}$, *называемых отображениями дешифрования;*

4. *каждому* $K \in \mathcal{K}$ *сопоставлены отображение шифрования* $e_K \in \mathcal{E}$ *и отображение дешифрования* $d_K \in \mathcal{D}$, *такие, что любого* $x \in \mathcal{P}$ *выполняется равенство* $d_K(e_K(x)) = x$.

ЗАМЕЧАНИЕ 1. В некоторых случаях предполагается, что заданы вероятностные распределения на множествах $\mathcal{P}$ и $\mathcal{K}$. Иначе говоря, предполагается, что символы открытого текста и выбираемые ключи шифртекста являются случайными величинами. Дальнейшие уточнения будут приведены ниже.

ЗАМЕЧАНИЕ 2. Множество $\mathcal{K}$ иногда называется пространством ключей или ключевым пространством.

ЗАМЕЧАНИЕ 3. В силу свойства 4, после шифрования символа шифртекста x отображением шифрования e_K и последующего дешифрования полученного шифртекста отображением d_K, получается исходный открытый текст.

ЗАМЕЧАНИЕ 4. В некоторых случаях множество $\mathcal{P}$ не совпадает с набором символов передаваемого сообщения. В ряде случаев эти символы кодируются тем или иным способом, например, неотрицательными числами из некоторого диапазона. В некоторых случаях в качестве множества $\mathcal{P}$ рассматриваются последовательности передаваемых символов (например, в обсуждаемом ниже шифре Виженера).

Выбрав криптосистему, отправитель и получатель используют следующий *протокол передачи данных*. Сначала случайным образом выбирается ключ K. Это делается, когда они находятся в одном месте, или же для выбора ключа используется *секретный* канал. В любом случае, эта информация не должна поступить в распоряжение противника. Затем отправи-

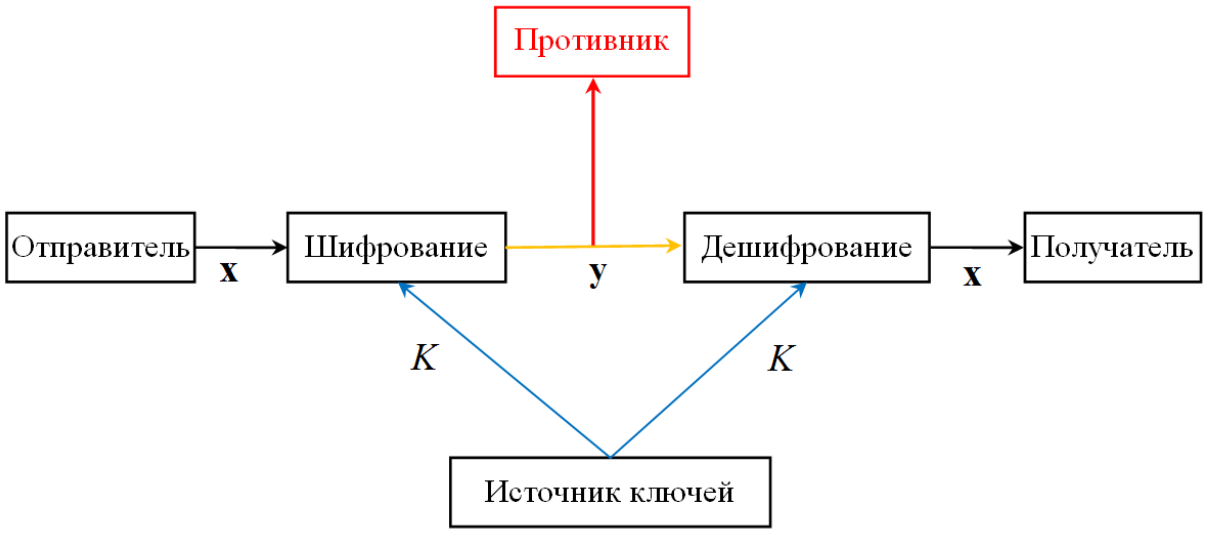
тель передает получателю информацию по основному *ненадежному* каналу. Предположим, что эта информация представляет собой строку

$$\mathbf{x} = x_1 x_2 \dots x_n,$$

где $n \geq 1$, $x_i \in \mathcal{P}$ для каждого i, $1 \leq i \leq n$. Каждый элемент этой строки шифруется с помощью отображения шифрования e_K, определяемого выбранным заранее ключом K. Это означает, что отправитель вычисляет значения $y_i = e_K(x_i)$, $1 \leq i \leq n$, и итоговая строка шифртекста

$$\mathbf{y} = y_1 y_2 \dots y_n$$

передается по каналу связи. Получатель, получивший это сообщение, дешифрует его с помощью отображения d_K и получает исходную строку открытого текста. Описанная схема изображена на рисунке.



На рисунке желтым цветом изображен ненадежный канал связи, а синим цветом — надежный канал.

Подчеркнем, что отображение шифрования e_K обязательно должно быть инъективным, иначе дешифрование может оказаться неоднозначным. Например, если $y = e_K(x_1) = e_K(x_2)$, причем $x_1 \neq x_2$, то получатель, получивший сообщение y, не сможет определить, каким было исходное сообщение. Напомним, что свойство 4 приведенного определения называется

обратимостью слева отображения e_K и равносильно именно его инъективности.

Заметим также, что в наиболее распространенном случае $\mathcal{P}=\mathcal{C}$ каждое отображение шифрования становится перестановкой. Иначе говоря, если множество открытых текстов и шифртекстов совпадают, то каждая функция шифрования просто переставляет элементы этого множества.

1.1. Модулярная арифметика и шифр сдвига

В этом разделе мы опишем *шифр сдвига,* основанный на *модулярной арифметике.*

Выберем произвольное целое число $m \geq 2$, которое будем называть модулем. Для произвольного целого числа a обозначим через $a \bmod m$ остаток от деления числа a на m. Предполагается, что остаток от деления принимает целые значения от нуля до $m-1$.

Замечание. Операция $a \bmod m$ присутствует в ряде языков программирования. При этом часто ее результат принадлежит множеству целых чисел в диапазоне от $-(m-1)$ до $m-1$, а знак совпадает со знаком числа a. Говоря более точно, результатом является число $(a \bmod m) \cdot \operatorname{sign} a$, где $a \bmod m$ — введенное нами значение, $\operatorname{sign} a$ — знак числа a.

Рассмотрим множество $\mathbb{Z}_m = \{0,1,2,\ldots,m-1\}$. В $\mathbb{Z}_m$ определим операции сложения и умножения, которые будем пока обозначать символами $\oplus$ и $\otimes$ соответственно, чтобы отличать их от «обычных» сложения и умножения:

$$a \oplus b = (a+b) \bmod m, \quad a \otimes b = (a\ )\bmod m, \quad a,b \in \mathbb{Z}_m.$$

Отметим, прежде всего, что результат этих операций принадлежит множеству $\mathbb{Z}_m$. Введенные операции называются сложением и умножением *по модулю* m, а возникающая при этом арифметика — *модулярной*.

Замечание 1. Для любых a, $b \in \mathbb{Z}_m$ их сумма $a+b$ в «обычном» смысле удовлетворяет условию $0 \leq a+b \leq 2m-2$. Если при этом выполняется неравенство $a+b \leq m-1$, то $(a+b) \bmod m = a+b$. Если выполняется неравенство $a+b \geq m$, то $(a+b) \bmod m = a+b-m$, так как выполняется неравенство $0 \leq a+b-m \leq m-2$. Поэтому возможно следующее альтерна-

тивное определение операции $\oplus$:

$$a \oplus b = \begin{cases} a+b, & \text{если } a+b \le m-1, \\ a+b-m, & \text{если } a+b \ge m \end{cases}$$

Замечание 2. Из равенства $a \otimes b = r$, a, b, $r \in \mathbb{Z}_m$ по определению остатка от деления вытекает, что имеет место равенство $ab = cm + r$ для некоторого целого c. Обратно, если имеет место равенство $ab = cm + r$, где c, $r \in \mathbb{Z}$, $0 \le r \le m-1$, то $a \otimes b = r$.

Легко проверить, что введенные операции обладают следующими свойствами.

1) Для любых a, $b \in \mathbb{Z}_m$ имеет место равенство $a \oplus b = b \oplus a$. Это свойство называется *коммутативностью* операции сложения в $\mathbb{Z}_m$.

2) Для любых a, b, $c \in \mathbb{Z}_m$ имеет место равенство

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

Это свойство называется *ассоциативностью* операции сложения в $\mathbb{Z}_m$.

3) Для любого $a \in \mathbb{Z}_m$ имеет место равенство $a \oplus 0 = a$.

4) Для любого $a \in \mathbb{Z}_m$ существует такой элемент $b \in \mathbb{Z}_m$, что

$$a \oplus b = 0.$$

Элемент b находится единственным образом, обозначается $b = -a$ и называется *противоположным* к элементу a (в $\mathbb{Z}_m$).

5) Для любых a, $b \in \mathbb{Z}_m$ имеет место равенство $a \otimes b = b \otimes a$. Это свойство называется *коммутативностью* операции умножения в $\mathbb{Z}_m$.

6) Для любых a, b, $c \in \mathbb{Z}_m$ имеет место равенство

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

Это свойство называется *ассоциативностью* операции умножения в $\mathbb{Z}_m$.

7) Для любого $a \in \mathbb{Z}_m$ имеет место равенство $a \otimes 1 = a$.

8) Для любых a, b, $c \in \mathbb{Z}_m$ имеет место равенство

$$(a \oplus b) \otimes c = (a \otimes b) \oplus (a \otimes c).$$

Это свойство называется свойством или законом *дистрибутивности*.

В алгебраических терминах, в силу свойств $1) - 8)$, говорят, что множество $\mathbb{Z}_m$ образует *конечное коммутативное кольцо с единицей.* Если учитывать только свойства 1)–4) (то есть принять во внимание только одну из двух операций, введенных в множестве $\mathbb{Z}_m$), то, снова используя термины общей алгебры, можно сказать, что $\mathbb{Z}_m$ является *конечной коммутативной абелевой группой* (относительно операции сложения по модулю m).

В $\mathbb{Z}_m$ введем операцию вычитания формулой:

$$a \ominus b = a \oplus (-b), \quad a, b \in \mathbb{Z}_m,$$

где $-b$ — элемент, противоположный к b в $\mathbb{Z}_m$.

Замечание. Легко доказать, что имеет место равенство

$$a \ominus b = (a - b) \bmod m.$$

Рассмотрим некоторый алфавит, из символов которого будут составляться сообщения. Предположим, что этот алфавит состоит из m символов. Например, в случае русского алфавита можно взять $m = 33$, в случае латинского — $m = 26$. Перенумеруем буквы рассматриваемого алфавита числами от 0 до $m - 1$. Таким образом, устанавливается взаимно-однозначное соответствие между буквами этого алфавита и элементами кольца $\mathbb{Z}_m$. Теперь полагаем: $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m$. Для $K \in \mathcal{K}$ определим отображения

$$e_K(x) = x \oplus K, \quad x \in \mathcal{P}, \quad d_K(y) = y \ominus K, \quad y \in \mathcal{C}.$$

Приведем теперь пример. Рассмотрим полный русский алфавит из 33 букв и сопоставим буквам числа от 0 до 32:

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

ПРИМЕР. Рассмотрим шифр сдвига с ключом $K = 7$ и открытый текст:

местовстречиизменитьнельзя

Каждую букву открытого текста заменяем соответствующим элементом кольца $\mathbb{Z}_{33}$. Получаем последовательность

$$13, 5, 18, \ldots, 32.$$

Каждый из элементов этой последовательности складываем в $\mathbb{Z}_{33}$ с ключом $K = 7$:

$$20, 12, 25, \ldots, 6$$

и заменяем полученные значения соответствующими буквами:

УЛШЩХИШЩЧЛЮППОУЛФПЩГФЛТГОЁ

Для дешифрования полученного сообщения получатель, прежде всего, преобразует текст в последовательность чисел, затем вычитает из каждого числа 7 (по модулю 33, или, что то же самое, прибавляет 26 по тому же модулю) и, наконец, переводит числа в соответствующие буквы.

ЗАМЕЧАНИЕ. В приведенном примере для большей наглядности шифртекст записан заглавными буквами, а открытый текст — строчные. Этот стиль будет применяться и в дальнейших примерах.

Практически используемые криптосистемы должны обладать некоторыми свойствами. Приведем здесь два таких свойства.

1. *Каждая функция шифрования и каждая функция дешифрования должны быть эффективно вычислимыми (за приемлемое время и с помощью приемлемых вычислительных ресурсов).*

2. *Противник, получивший шифртекст* $\mathbf{y}$*, не должен быть в состоянии определить использованный ключ* K *или открытый текст* $\mathbf{x}$.

Процесс нахождения ключа K (или открытого текста $\mathbf{x}$) по задан-

ному шифртексту **y** называется *криптоанализом*, а противник, занимающийся криптоанализом — *криптоаналитиком*. Если противник найдет ключ K, то он сможет дешифровать **y**, используя отображение d_K. Следовательно, нахождение ключа K по меньшей мере так же сложно, как и нахождение открытого текста **x**.

Заметим, что шифр сдвига не является безопасным, поскольку он может быть подвергнут криптоанализу путем *исчерпывающего поиска ключей.* Поскольку количество возможных ключей невелико, легко испробовать все отображения дешифрования, и выбрать из всех вариантов осмысленный текст.

ПРИМЕР. Предположим, что имеется шифртекст, полученный с помощью шифра сдвига с неизвестным ключом

ДФАЬЭПНФОЛЩРКНЧКРЮЭКМРУЪЫЛЭЩЖШ

Применяем к нему отображения *дешифрования* d_0, d_1, $d_2 \ldots$. Получаем следующие строки:

$K = 0$ **дфаьэпнфолщркнчкрюэкмруъылэщжш**

$K = 1$ **гуяыьомункшпймцйпэьйлптщъкьшёч**

$K = 2$ **втюъынлтмйчоилхиоьыикосшщйычец**

$K = 3$ **бсэщъмкслицнзкфзныъзйнрчшиъцдх**

$K = 4$ **арьшцлйркзхмжйужмъщжимпцчзщхгф**

$K = 5$ **япычшкипйжфлёитёлщшёзлохцжшфву**

$K = 6$ **юоъцчйзоиёукезсекшчежкнфхёчубт**

$K = 7$ **энщхцижнзетйджрдйчцдёймуфецтас**

$K = 8$ **ьмшфхзёмждсигёпгицхгеилтудхсяр**

$K = 9$ **ылчуфжелёгрзвеовзхфвдзкстгфрюп**

$K = 10$ **ъкцтуёдкевпжбднбжфубгжйрсвупэо**

$K = 11$ **щйхстегйдбоёагмаёутавёипрбтоьн**

$K = 12$ **шифрсдвиганеявляетсябезопасным**

Мы получили осмысленный текст, и можем остановиться. Итак, использовался ключ $K = 12$.

Ясно, что в данном случае (33 символа) *при равновероятном выборе ключей* математическое ожидание числа попыток дешифрования равно 16.5.

Приведенный пример позволяет высказать следующее простейшее необходимое требование к безопасности криптосистемы: исчерпывающий перебор ключей должен быть неосуществимым, то есть пространство ключей должно быть очень велико. Разумеется, и это условие не гарантирует безопасность.

1.2. Шифр подстановки

Другой элементарной криптосистемой является шифр подстановки. Дадим формальное описание этой системы.

Пусть $\mathcal{A}$ — некоторый алфавит. Полагаем $\mathcal{P}=\mathcal{C}=\mathcal{A}$, $\mathcal{K}$ состоит из всех *подстановок* на множестве $\mathcal{A}$, то есть взаимно-однозначных отображений $\mathcal{A}$ на $\mathcal{A}$. Для каждой подстановки $\varphi\in\mathcal{K}$ полагаем

$$e_\varphi(x)=\varphi(x),\quad x\in\mathcal{P};\quad d_\varphi(y)=\varphi^{-1}(y),\quad y\in\mathcal{C},$$

где φ^{-1} — подстановка, обратная к φ.

Если алфавит $\mathcal{A}$ состоит из m элементов, то число подстановок на множестве $\mathcal{A}$, то есть число элементов множества $\mathcal{K}$, равно $m!$. Уже при значениях m, равных числу символов в упоминаемых нами русском и латинском алфавитах, значение $m!$ очень велико. Например,

$$26!\approx 4.0329\times 10^{26},\quad 33!\approx 8.6833\times 10^{36}.$$

Следовательно, исчерпывающий перебор всех возможных ключей в данном случае уже практически неосуществим. Однако как мы покажем ниже, шифр подстановки легко поддается криптоанализу другими методами.

Рассмотрим пример случайно выбранной перестановки, которую можно использовать в качестве отображения шифрования (как и выше, символы открытого текста записываются строчными буквами, а символы шифртекста — заглавными).

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
Й	Ц	У	К	Е	Н	Г	Ш	Щ	З	Х	Ъ	Ф	Ы	В	А

п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
П	Р	О	Л	Д	Ж	Э	Я	Ч	С	М	И	Т	Ь	Б	Ю	Ё

Таким образом, e_φ(а) = Й, e_φ(б)=Ц, и так далее.


В качестве упражнения читателю предлагается дешифровать следующий текст, зашифрованный с помощью приведенной выше подстановки:

СЗЖРПАЕОЛЙВАУЪЗВНЁУФЁНЛОЁВЙЕНШВТЫ

1.3. Некоторые сведения из теории чисел. Аффинный шифр

Шифр сдвига является частным случаем шифра подстановки, использующим алфавит, составленный из m символов. При этом из возможных $m!$ ключей используются только m. Другим частным случаем шифра подстановки является *аффинный шифр.* Сначала приведем кратко некоторые вспомогательные определения и утверждения.

ОПРЕДЕЛЕНИЕ. Пусть a, $b \in \mathbb{Z}$, причем $b \neq 0$. Говорят, что число b делит число a, если существует целое число c, такое, что $a = bc$. В этом случае говорят также, что число b является делителем числа a и пишут $b \mid a$.

ОПРЕДЕЛЕНИЕ. Пусть a, b, $d \in \mathbb{Z}$ и $d \neq 0$. Если $d \mid a$, $d \mid b$, то число d называется общим делителем чисел a и b.

ОПРЕДЕЛЕНИЕ. Предположим, что целые числа a, b не равны нулю одновременно. Число $d \geq 1$ называется наибольшим общим делителем чисел a, $b \in \mathbb{Z}_m$, если $d \mid a$, $d \mid b$ и число d делится на любой общий делитель чисел a и b.

Справедливо следующее утверждение.

Наибольший общий делитель двух чисел a, b не равных нулю одновременно, существует и находится единственным образом.

ЗАМЕЧАНИЕ. В некоторых случаях в определение наибольшего общего делителя не включается требование, чтобы он был положительным. Тогда наибольший общий делитель находится однозначно с точностью до множителя ± 1, то есть если d удовлетворяет указанному определению, то $-d$ также будет ему удовлетворять и других чисел, удовлетворяющих определению, не будет.

Обозначим наибольший общий делитель чисел a и b через (a,b). Этот наибольший общий делитель может быть найден с помощью так называемого алгоритма Евклида, который мы запишем в следующей рекурсивной форме. В силу очевидных соотношений $(a,b)=(\pm a,\pm b)$, выполняющихся для любых комбинаций знаков, можно ограничиться предположением, что числа a и b являются неотрицательными. Тогда алгоритм нахождения наибольшего общего делителя выглядит так:

1) Если $a=0$, то $(a,b)=b$.

2) Если $b=0$, то $(a,b)=a$.

3) $(a,b)=(b,a \bmod b)$.

ОПРЕДЕЛЕНИЕ. Числа a и b называются взаимно простыми, если $(a,b)=1$.

Очевидно, что взаимная простота двух чисел равносильна тому, что у них нет общего делителя, большего единицы.

Можно доказать такое свойство взаимно простых чисел, которое будет использовано ниже: если $c \mid ab$ и числа c и a взаимно простые, то $c \mid b$.

Вернемся теперь к анализу кольца $\mathbb{Z}_m$.

ОПРЕДЕЛЕНИЕ. Элемент $a \in \mathbb{Z}_m$ называется обратимым, если существует такой элемент $b \in \mathbb{Z}_m$, что $a \otimes b = 1$.

Если элемент a обратим, то элемент b, удовлетворяющий условию предыдущего определения, находится единственным образом, называется обратным к элементу a и обозначается $b = a^{-1}$.

Рассмотрим, например, кольцо $\mathbb{Z}_5$. В этом кольце выполняется равенство $2 \otimes 3 = 1$. Отсюда следует, что элемент 2 обратим в данном кольце и $2^{-1} = 3$. Разумеется, обратим и элемент 3 и $3^{-1} = 2$.

ТЕОРЕМА 1. *Элемент $a \in \mathbb{Z}_m$ обратим в кольце $\mathbb{Z}_m$ в том и только том случае, когда числа a и m являются взаимно простыми.*

ДОКАЗАТЕЛЬСТВО. 1) Предположим, что элемент $a \in \mathbb{Z}_m$ обратим. Соотношение $a \otimes b = 1$ равносильно равенству $(ab) \bmod m = 1$, которое, в свою очередь, означает, что существует такое целое число c, что $ab = cm + 1$, то есть $ab - cm = 1$. Предположим, что натуральное число d является общим делителем чисел a и m. Тогда $d \mid (ab - cm)$, и из последнего равенство получаем, что $d \mid 1$. Следовательно, $d = 1$. Мы доказали, что числа a и m взаимно простые.

2) Предположим, что числа a и m взаимно простые, и докажем, что элемент a обратим в кольце $\mathbb{Z}_m$. Умножим элемент a последовательно на все элементы кольца $\mathbb{Z}_m$:

$$a \otimes 0, \quad a \otimes 1, \ldots, a \otimes (m-1). \qquad (*)$$

Последовательность $(*)$ содержит m элементов кольца $\mathbb{Z}_m$. Покажем, что все выписанные произведения попарно различны. Отсюда будет следовать, среди этих элементов присутствуют *все* элементы кольца $\mathbb{Z}_m$, поскольку само кольцо содержит m элементов. Следовательно, одно из этих произведений $(*)$ равно элементу 1. Тем самым, доказательство будет завершено.

Допустим, что для некоторых k, $l \in \mathbb{Z}_m$ выполняется равенство

$$a \otimes k = a \otimes l.$$

Обозначим это произведение через r. Тогда для некоторых c_1, c_2 имеем:

$$ak = c_1 m + r, \quad al = c_2 m + r.$$

Вычитаем из первого равенства второе: $a(k-l) = (c_1 - c_2)m$. Число m делит правую часть равенства. Следовательно, оно делит его левую часть. Но числа a и m взаимно простые. Поэтому из соотношения $m \mid a(k-l)$ следует, что $m \mid (k-l)$. Из условий $0 \le k \le m-1$, $0 \le l \le m-1$ получаем, что

$$-(m-1) \le k - l \le m - 1.$$

Среди чисел последовательности

$$-(m-1), -(m-2), \ldots, -2, -1, 0, 1, 2, \ldots, m-2, m-1$$

на m делится только число 0. Поэтому из соотношения $m|(k-l)$ следует, что $k-l=0$, то есть $k=l$, то есть последовательность $(*)$ не содержит одинаковых элементов.

Теорема доказана.

ТЕОРЕМА 2. *Пусть* $a \in \mathbb{Z}_m$. *Отображение* $f(x)=a\otimes x$, *действующее из* $\mathbb{Z}_m$ *в* $\mathbb{Z}_m$ *является обратимым в том и только том случае, когда элемент* a *обратим в* $\mathbb{Z}_m$.

ДОКАЗАТЕЛЬСТВО. Предположим, что элемент a обратим в $\mathbb{Z}_m$. Тогда отображение $g(x)=a^{-1}\otimes x$ является обратным к f. Действительно, для любого $x\in\mathbb{Z}_m$

$$g(f(x))=a^{-1}\otimes(a\otimes x)=(a^{-1}\otimes a)\otimes x=1\otimes x=x.$$

Аналогично проверяем, что $f(g(x))=x$ для любого $x\in\mathbb{Z}_m$.

Допустим, что отображение f обратимо. Обозначим $g=f^{-1}$. Тогда для любого $x\in\mathbb{Z}_m$ выполняется равенство $f(g(x))=x$, то есть

$$a\otimes g(x)=x.$$

Полагая $x=1$, отсюда получаем: $a\otimes g(1)=1$, элемент a обратим.

Теорема доказана.

СЛЕДСТВИЕ. *Пусть* a, $b\in\mathbb{Z}_m$. *Отображение* $f(x)=a\otimes x\oplus b$, *действующее из* $\mathbb{Z}_m$ *в* $\mathbb{Z}_m$ *является обратимым в том и только том случае, когда элемент* a *обратим в* $\mathbb{Z}_m$.

ДОКАЗАТЕЛЬСТВО. Введем два отображения g и h действующие из $\mathbb{Z}_m$ в $\mathbb{Z}_m$ по формулам: $g(x)=a\otimes x$, $h(x)=x\oplus b$. Очевидно, что выполняется равенство $f(x)=h(g(x))$, $x\in\mathbb{Z}_m$. Отображение h будет обратимым при любом значении b. Следовательно, отображения f и g являются об-

ратимыми или нет одновременно. Остается воспользоваться теоремой 2.

Следствие доказано.

В дальнейшем бы будем обозначать операции по модулю m как обычные сложение и умножение, уточняя, что операции выполняются именно в модулярной арифметике.

Перейдем к определению аффинного шифра.

Здесь мы снова будем предполагать, что $\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$. Пусть

$$\mathcal{K} = \{(a,b) : a,b \in \mathbb{Z}_m, \quad (a,m) = 1\}.$$

Для $K = (a,b) \in \mathcal{K}$ определим отображения e_K и d_K формулами

$$e_K(x) = a \cdot x + b, \quad x \in \mathbb{Z}_m, \quad d_K(y) = a^{-1}(y-b), \quad y \in \mathbb{Z}_m,$$

где все операции выполняются в кольце $\mathbb{Z}_m$. В силу следствия теоремы 2, отображение e_K, действующее в $\mathbb{Z}_m$, является обратимым при любом $K \in \mathcal{K}$. Очевидно, что для любого $x \in \mathbb{Z}_m$ выполняется соотношение $d_K(e_K(x)) = x$.

ПРИМЕР. Рассмотрим русский алфавит из 33 букв и, как и выше, отождествим эти буквы с элементами кольца $\mathbb{Z}_{33}$. Пусть $a = 7$, $b = 3$. Числа $a = 7$ и $m = 33$ являются взаимно простыми, то есть пару $(7,3)$ можно рассматривать в качестве ключа. Непосредственной проверкой убеждаемся в том, что $a^{-1} = 19$. Тогда функции шифрования и дешифрования в данном случае имеют вид:

$$e_K(x) = 7x + 3, \quad x \in \mathbb{Z}_{33}; \quad d_K(y) = 19(y-3) = 19y + 9, \quad y \in \mathbb{Z}_{33}.$$

Тогда, например, буква **«д»** шифруется так:

$$\text{«д»} \Rightarrow 4 (\in \mathbb{Z}_{33}) \Rightarrow e_K(4) = 7 \times 4 + 3 = 31 (\in \mathbb{Z}_{33}) \Rightarrow \text{«ю»}.$$

Легко проверить, что открытому тексту

аффинныйшифрявляетсячастнымслучаемшифраподстановки

будет соответствовать шифртекст:

ГССАВВБЖМАСЦЬРФЬЕДЭЬЁГЭДВБЫЭФКЁГЕЫМАСЦГПИЮЭДГВИРНА

Читателю предоставляется проверить, что отображение d_K переводит этот шифртекст в исходный открытый текст.

В заключение рассмотрим вопрос о размере ключевого пространства аффинного шифра. Приведем сначала некоторые важные факты из теории чисел.

Напомним, что число $p>1$ называется простым, если оно не имеет натуральных делителей, отличных от 1 и p. Известно, что любое натуральное число $n>1$ допускает разложение вида $n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$, где числа p_1, p_2, …, p_r являются простыми, а числа k_1, k_2, …, k_r — натуральными. Указанное разложение определяется числом n однозначно с точностью до порядка следования множителей и называется *каноническим разложением* числа n.

ОПРЕДЕЛЕНИЕ. Функция Эйлера φ определяется на множестве всех натуральных чисел следующим образом: $\varphi(1)=1$, при $n>1$ значение $\varphi(n)$ равно количеству всех чисел в последовательности 1, 2, …, $n-1$, взаимно простых с n.

ЗАМЕЧАНИЕ. Иногда в литературе дается несколько иное определение функции Эйлера: для любого $n\geq 1$ $\varphi(n)$ равно количеству всех чисел в последовательности 0, 1, 2, …, $n-1$, взаимно простых с n. При $n=1$ выписанная последовательность состоит из одного числа 0, которое взаимно просто с $n=1$. При $n>1$ числа 0 и n не являются взаимно простыми, поэтому при подсчета количества чисел, взаимно простых с n число 0 можно исключить, и мы приходим к приведенному выше определению.

Найдем несколько значений функции Эйлера. В каждой строке сначала будет указано число n, затем последовательность чисел 1, 2, …, $n-1$. Числа, не являющиеся взаимно простыми с n, будут выделены цве-

том. Затем указывается значение функции Эйлера.

$n=2$, 1, $\varphi(2)=1$,

$n=3$, 1, 2, $\varphi(3)=2$,

$n=4$, 1, 2, 3, $\varphi(4)=2$,

$n=5$, 1, 2, 3, 4, $\varphi(5)=4$,

$n=6$, 1, 2, 3, 4, 5, $\varphi(6)=2$,

$n=7$, 1, 2, 3, 4, 5, 6, $\varphi(7)=6$,

$n=8$, 1, 2, 3, 4, 5, 6, 7, $\varphi(8)=4$.

Отметим следующий факт: если число p простое, то $\varphi(p)=p-1$. Действительно, в этом случае все числа последовательности $1, 2, \ldots, p-1$ являются взаимно простыми с числом p. Легко показать, что если число p простое, то для любого натурального k имеет место равенство

$$\varphi(p^k)=p^k-p^{k-1}.$$

Отметим следующее важное свойство функции Эйлера: *для любых натуральных и взаимно простых чисел* m *и* n *имеет место равенство*

$$\varphi(mn)=\varphi(m)\varphi(n).$$

Из отмеченных свойств вытекает формула для нахождения значения функции Эйлера: если число $n>1$ имеет каноническое разложение

$$n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r},$$

то

$$\varphi(n)=(p_1^{k_1}-p_1^{k_1-1})(p_2^{k_2}-p_2^{k_2-1})\ldots(p_r^{k_r}-p_r^{k_r-1}).$$

Вынося из каждой скобки первое слагаемое, получаем следующую формулу для нахождения значения функции Эйлера, которая часто фигурирует в литературе:

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).$$

Вернемся теперь к аффинному шифру. Его ключ имеет вид $K=(a,b)$, где $0\le a\le m-1,\ (a,m)=1,\ 0\le b\le m-1$. Таким образом, элемент a может принимать $\varphi(m)$ значений, а элемент b может принимать m значений. Следовательно, общее число различных ключей равно $m\varphi(m)$.

1.4. Шифр Виженера

Начиная с этого раздела мы будем обозначать операции в кольце $\mathbb{Z}_m$ как обычные сложение, вычитание и умножение, добавляя в случае необходимости, что операции выполняются в указанном кольце.

В шифре сдвига и шифре подстановки после выбора ключа каждый символ алфавита переводится при шифровании в однозначно определенный символ. По этой причине такие шифры называются *моноалфавитными*. Рассматриваемый в этом пункте *шифр Виженéра*[1] не является моноалфавитным.

Как и выше, отождествим буквы рассматриваемого алфавита с элементами кольца $\mathbb{Z}_m$. Выберем и зафиксируем некоторое натуральное число l. Полагаем $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^l$. Для произвольного ключа

$$K = (k_1, k_2, \ldots, k_l)$$

введем отображения $e_K : \mathcal{P} \to \mathcal{C}$ и $d_K : \mathcal{C} \to \mathcal{P}$ следующим образом:

$$e_K(x_1, x_2, \ldots, x_l) = (x_1 + k_1, x_2 + k_2, \ldots, x_l + k_l),$$

$$d_K(y_1, y_2, \ldots, y_l) = (y_1 - k_1, y_2 - k_2, \ldots, y_l - k_l),$$

где все операции выполняются по модулю m.

В данном случае ключ является строкой длины l и называется *ключевым словом.* Шифр Виженера зашифровывает одновременно l алфавитных символов.

Пример. Рассмотрим русский алфавит, состоящий из 33 букв, отождествленных с элементами кольца $\mathbb{Z}_{33}$. Предположим, что $l = 6$, в качестве ключевого слова возьмем слово **СКРЫТЬ**, имеющее следующий экви-

[1] Блез де Виженéр — придворный французского короля Генриха III, жил в 16 столетии. На протяжении почти трехсот лет шифр Виженера считался практически не взламываемым.

валент в $\mathbb{Z}_{33}$:

$$K = (18, 11, 17, 28, 19, 29).$$

В качестве открытого текста возьмем строку

шифрвиженератакженеявляетсянадежным

Переведем символы открытого текста в элементы кольца $\mathbb{Z}_{33}$, разобьем их на группы по шесть элементов и сложим в каждой группе с соответствующими элементами ключевого слова:

	25	9	21	17	2	9	7	5	14	5	17	0	19	0
+	18	11	17	28	19	29	18	11	17	28	19	29	18	11
=	10	20	5	12	21	5	25	16	31	0	3	29	4	11

	11	7	5	14	5	32	2	12	32	5	19	18	32	14
+	17	28	19	29	18	11	17	28	19	29	18	11	17	28
=	28	2	24	10	23	10	19	7	18	1	4	29	16	9

	0	4	5	7	14	28	13
+	19	29	18	11	17	28	19
=	19	0	23	18	31	23	32

В приведенной выше таблице группы, состоящие из шести элементов, выделены разными цветами.

Алфавитным эквивалентом полученной строки будет следующая:

ЙУЕЛФЕШПЮАГЬДКЫВЧЙЦЙТЖСБДЬПИТАЦСЮЦЯ

В общем случае алфавита, составленного из m букв и ключевого слова длины l число различных ключей равно m^l. В частности, при $m = 33$ (полный русский алфавит) и $l = 6$ число ключей приближенно равно 1.2915×10^9. Это уже достаточно много для исчерпывающего перебора вручную (но не на компьютере).

В случае шифра Виженера с ключевым словом длины l каждый символ алфавита может отображаться в один из l символов алфавита (в предположении, что все буквы ключевого слова различны). Такая криптосистема называется полиалфавитной.

1.5. Шифр Хилла

В этом разделе мы опишем другую полиалфавитную криптосистему, называемую шифром Хилла. Этот шифр был изобретен в 1929 году Л.С. Хиллом.

Приведем сначала некоторые предварительные сведения о матрицах с элементами из кольца $\mathbb{Z}_m$. Выберем и зафиксируем некоторое натуральное число n. Рассмотрим матрицу $A=(a_{ij})_{i,j=1}^{n}$ с элементами из $\mathbb{Z}_m$. Для этих матриц вводятся операции сложения и умножения по обычным правилам действий с матрицами с тем отличием, что действия с элементами выполняются по правилам кольца $\mathbb{Z}_m$. Вводится понятие единичной матрицы, произведения матриц (которое мы будем обозначать, как и произведение «обычных» числовых матриц), обратимой матрицы и понятие определителя. При этом сохраняются все основные свойства действий с матриц и определителей матриц. В частности, остается в силе утверждение об определителе произведения матриц, которое будем записывать следующим образом: $|AB|=|A|\cdot|B|$, где произведение в правой части понимается в смысле кольца $\mathbb{Z}_m$.Отметим также, что определитель матрицы с элементами из кольца $\mathbb{Z}_m$ можно найти следующим образом: сначала найти определитель матрицы, считая ее элементы целыми числами, то есть выполняя обычные операции с числами, а затем взять остаток от деления полученного числа на m.

Критерий обратимости матрицы выглядит в этом случае так: *квадратная матрица с элементами из кольца* $\mathbb{Z}_m$ *обратима в том и только том случае, когда ее определитель взаимно прост с числом* m. Действительно, допустим, что матрица A обратима. Тогда имеет место равенство

$$AA^{-1} = E,$$

где E — единичная матрица. Переходя к определителям матриц (являющимся элементами кольца $\mathbb{Z}_m$), получаем:

$$|AA^{-1}| = |E|, \quad |A| \cdot |A^{-1}| = 1.$$

Последнее равенство означает, что элемент $|A|$ обратим в кольце $\mathbb{Z}_m$.

Обратное утверждение можно доказать по стандартной схеме, применяемой в случае числовых матриц, и мы не будем на этом останавливаться.

По аналогии с произведением квадратных матриц с элементами из кольца $\mathbb{Z}_m$ можно ввести произведение произвольных матриц с такими элементами.

Отождествляем буквы рассматриваемого алфавита с элементами кольца $\mathbb{Z}_m$. Выберем и зафиксируем некоторое натуральное число n. Полагаем $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^n$. В качестве множества ключей $\mathcal{K}$ возьмем множество всех *обратимых* квадратных матрица порядка n с элементами из кольца $\mathbb{Z}_m$. Для $K \in \mathcal{K}$ полагаем

$$e_K(x) = xK, \quad x \in \mathcal{P}; \quad d_K(y) = yK^{-1}, \quad y \in \mathcal{C}.$$

Поясним приведенные формулы. Элемент $x \in \mathcal{P}$ можно рассматривать как вектор-строку длины n. После умножения такого вектора справа на матрицу K по правилам матричного умножения мы снова получаем вектор-строку такого же типа. Пользуясь стандартными свойствами теории определителей, легко убедиться в том, что инъективность отображения e_K (которое можно определить и без предположения об обратимости матрицы K) равносильна обратимости этой матрицы.

Пример. Пусть $m = 33$, $n = 3$. Рассмотрим матрицу с элементами из кольца $\mathbb{Z}_{33}$:

$$K = \begin{pmatrix} 1 & 3 & 17 \\ 10 & 6 & 3 \\ 2 & 4 & 5 \end{pmatrix}.$$

Ее определитель в кольце $\mathbb{Z}_{33}$ равен 32 (можно сначала найти определитель матрицы, считая все ее элементы целыми числами, этот определитель равен 362, а затем найти остаток от деления полученного числа на 33). Числа 32 и 33 взаимно простые. Следовательно, рассматриваемая матрица обратима (в кольце матриц с элементами из $\mathbb{Z}_{33}$). Непосредственной проверкой убеждаемся в том, что

$$K^{-1} = \begin{pmatrix} 15 & 13 & 27 \\ 11 & 29 & 31 \\ 5 & 31 & 24 \end{pmatrix}.$$

С помощью шифра Хилла с рассматриваемым ключом K зашифруем следующий текст:

шифрованиепометодухиллаиспользуетматричноеумножение

Разбиваем текста на группы по три элемента, преобразуем их в соответствующие элементы кольца $\mathbb{Z}_{33}$, умножаем (в $\mathbb{Z}_{33}$) полученную вектор-строку справа на матрицу K и, наконец, находим соответствующие буквы алфавита. Например, первые три буквы преобразуются так:

$$\text{"шиф"} \Rightarrow (25,\ 9,\ 21) \Rightarrow (25,\ 9,\ 21)\begin{pmatrix} 1 & 3 & 17 \\ 10 & 6 & 3 \\ 2 & 4 & 5 \end{pmatrix} =$$

$$= (25,\ 15,\ 12) \Rightarrow \text{"ЬЪ}\ldots\text{"}$$

Предоставляем читателю убедиться в том, что вся исходная строка преобразуется так:

ШОЬЁРНЩФФЭЁЙВМБЬРДДГЯЭЁСЙЛАФКБИБФСПТЦГЖИУКМЬУЬЗДОРЩ

Можно найти число различных ключей в случае шифра Хилла, но мы не будем на этом останавливаться. Детальное рассмотрение этого во-

проса содержится в следующей статье: Jeffrey Overbey, William Traves, and Jerzy Wojdylo, On the Keyspace of the Hill Cipher, Cryptologia, 29 (1), January 2005, pp. 59 – 72.

1.6. Шифр перестановки

Все описанные выше криптосистемы используют подстановки: буквы открытого текста в шифртексте заменяются другими буквами. Идея шифра перестановки заключается в том, чтобы оставить сами буквы открытого текста без изменения, изменив лишь их позиции. Как и в случае шифра подстановки, здесь удобнее использовать сам исходный алфавит, а не кольцо $\mathbb{Z}_m$, поскольку никаких алгебраических операций над элементами не производится.

Схема шифрования такова. Выбираем некоторое $n>1$ и произвольную перестановку из n элементов. Разбиваем строку открытого текста на группы из n символов и переставляем их в соответствии с выбранной перестановкой.

ПРИМЕР. Пусть $n=6$, рассмотрим следующую перестановку из шести элементов: 3, 1, 5, 6, 4, 2. Тогда последовательность **абвгде** преобразуется в последовательность **ВАДЕГБ**. Дешифрование происходит по той же схеме с помощью перестановки 2, 6, 1, 5, 3, 4.

Общая схема шифрования выглядит так. Пусть $\mathcal{A}$ — рассматриваемый алфавит. Тогда $\mathcal{P}=\mathcal{C}=\mathcal{A}^n$, в качестве множества ключей $\mathcal{K}$ берется множество $\mathfrak{S}_n$ всех *подстановок* степени n, то есть взаимно-однозначных отображений множества $\{1,2,\ldots,n\}$ на себя. Тогда для $\varphi\in\mathcal{K}$ отображения e_φ и d_φ, определенные на последовательностях длины n символов из алфавита $\mathcal{A}$, определены так:

$$e_\varphi:(x_1,x_2,\ldots,x_n)\mapsto(x_{\varphi(1)},x_{\varphi(2)},\ldots,x_{\varphi(n)}),$$

$$d_\varphi:(y_1,y_2,\ldots,y_n)\mapsto(y_{\varphi^{-1}(1)},y_{\varphi^{-1}(2)},\ldots,y_{\varphi^{-1}(n)}),$$

где φ^{-1} — подстановка, обратная к φ.

В частности, в рассмотренном выше примере

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 6 & 4 & 2 \end{pmatrix}, \quad \varphi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 3 & 4 \end{pmatrix}.$$

Заметим, что вторые строки в приведенных таблицах — *перестановки* шифрования и дешифрования.

Шифр перестановки является частным случаем шифра Хилла. Действительно, сопоставим произвольной перестановке $\varphi \in \mathfrak{S}_n$ *матрицу подстановки* $K_\varphi = (k_{ij})$ — квадратную матрицу порядка n, элементы которой определяются формулой

$$k_{ij} = \begin{cases} 1, \text{если} \quad (\varphi) i = j \\ 0 \text{в противном случае.} \end{cases}$$

ЗАМЕЧАНИЕ. В каждой строке и в каждом столбце матрицы подстановки один из элементов равен единице, а остальные равны нулю. Матрица подстановки K_φ может быть получена из единичной матрицы порядка n путем выписывания ее строк в порядке $\varphi(1), \varphi(2), \ldots, \varphi(n)$ или столбцов в порядке $\varphi^{-1}(1), \varphi^{-1}(2), \ldots, \varphi^{-1}(n)$. Легко убедиться в том, что для обращения матрицы подстановки достаточно ее *транспонировать*.

Имеет место равенство $K_\varphi^{-1} = K_{\varphi^{-1}}$, то есть матрица, обратная к *матрице* подстановки, является матрицей подстановки, соответствующей *обратной подстановке*. Таким образом, и дешифрование рассматриваемого шифра по алгоритму шифра Хилла эквивалентно его дешифрованию как шифра перестановки.

Для указанной выше подстановки φ соответствующие матрицы имеют вид:

$$K_{\varphi} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad K_{\varphi^{-1}} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Глава 2. Криптоанализ

2.1. Предварительные сведения

Перейдем теперь к обсуждению методов криптоанализа. Обычно делается предположение, называемое *принципом Керкгоффса*, о том, что криптоаналитик (противник, нарушитель) знает используемую криптосистему.

Выделим сначала основные виды *атак* на криптосистему. Во всех случаях предполагается, что противник знает алгоритм шифрования, *но не ключ*.

Криптоанализ на основе шифртекста

Противнику доступна строка шифртекста **y**. Это возможно в случае, когда противник имеет доступ к каналу связи.

Криптоанализ на основе открытого текста

Противник получает в свое распоряжение строку открытого текста **x** и соответствующую строку шифртекста **y**.

Криптоанализ на основе выбранного открытого текста

Противник может *выбрать* строку открытого текста **x** и получить соответствующую строку шифртекста **y**. Это возможно в случае, когда противник имеет временный доступ к аппаратуре шифрования.

Криптоанализ на основе выбранного шифртекста

Противник может *выбрать* строку шифртекста **y** и получить соответствующую строку открытого текста **x**. Это возможно в случае, когда противни имеет временный доступ к аппаратуре дешифрования.


В каждом случае задача криптоаналитика состоит в нахождении ключа шифрования. Очевидно, что приведенные четыре вида атак находятся в порядке возрастания степени их благоприятности для нападающего.

Рассмотрим сначала самый слабый тип атаки — на основе шифртекста. Будем предполагать, что открытый текст представляет собой обычный русский текст без знаков препинания и пробелов (по сравнению со случаем, когда шифруются знаки препинания и пробелы, это более сложная задача). Будем также предполагать, что текст не использует букву **"ё"**, вместо которой пишется буква **"е"**. Иначе говоря, будет использоваться алфавит, содержащий 32 буквы.

В приводимой ниже таблице находятся относительные частоты (вероятности появления) букв. Из этой таблицы видно, что

1) буква **"о"** имеет вероятность около **0.11**;

2) буквы **"е"** и **"а"** имеют вероятности около **0.8**;

3) буквы **"и"** и **"н"** имеют вероятности около **0.7**, и так далее.

Буква	Вероятность	Буква	Вероятность
а	0.079183	р	0.044470
б	0.017063	с	0.053261
в	0.043270	т	0.061753
г	0.017402	у	0.027981
д	0.030460	ф	0.001879
е	0.084100	х	0.008934
ж	0.010468	ц	0.003616
з	0.017532	ч	0.014690
и	0.068290	ш	0.008142
й	0.011231	щ	0.003721
к	0.033586	ъ	0.000247

Буква	Вероятность	Буква	Вероятность
л	0.050010	ы	0.019640
м	0.032575	ь	0.019197
н	0.067195	э	0.003844
о	0.110789	ю	0.006050
п	0.028097	я	0.021324

Таблица 1,

частотные характеристики букв русского языка

Для частотного криптоанализа анализа важными являются также *биграммы* и *триграммы*, то есть группы по две и три буквы. Приведем тридцать биграмм в русском языке, имеющих наибольшую вероятность (приблизительно от **0.014834** до **0.007073**):

"то", "ст", "но", "на", "по", "не", "ен", "ов",

"ко", "ни", "он", "ос", "ал", "ра", "от", "ли",

"ро", "ер", "го", "ка", "пр", "ол", "во", "ет",

"ес", "ре", "ло", "ан", "ор", "ом".

Заметим, что количество (формально возможных) биграмм в данном случае равно $32^2 = 1024$. С этим связана существенно меньшая вероятность наиболее вероятной биграммы по сравнению с наиболее вероятной буквой.

Тридцать триграмм в русском языке, имеющих наибольшую вероятность (приблизительно от **0.003474** до **0.001723**) следующие:

"ост", "что", "про", "его", "ени", "ого",

"ста", "ать", "ото", "при", "ест", "енн",

"это", "сто", "аза", "ств", "тор", "оро",

"ере", "оль", "как", "она", "ова", "был",

"али", "лся", "все", "вер", "тел", "льн".

Приведем аналогичные характеристики для букв английского языка.

Буква	Вероятность	Буква	Вероятность
a	0.081716	n	0.068793
b	0.015979	o	0.076513
c	0.027389	p	0.018749
d	0.041704	q	0.001112
e	0.122352	r	0.060362
f	0.022916	s	0.063354
g	0.021081	t	0.089239
h	0.058286	u	0.028798
i	0.068545	v	0.010077
j	0.001982	w	0.021125
k	0.008695	x	0.001781
l	0.043247	y	0.019296
m	0.025913	z	0.000996

Таблица 2,

частотные характеристики букв английского языка

Тридцать биграмм в английском языке, имеющих наибольшую вероятность (приблизительно от **0.029955** до **0.007396**) следующие:

"th", "he", "in", "er", "an", "re", "es", "nd",

"st", "on", "en", "ea", "at", "ed", "nt", "ha",

"to", "or", "ou", "ng", "et", "it", "ar", "te",

"is", "ti", "hi", "as", "of", "se".

Тридцать триграмм в английском языке, имеющих наибольшую вероятность (приблизительно от **0.018442** до **0.002167**) следующие:


"the", **"and"**, **"ing"**, **"her"**, **"tha"**, **"ere"**,
"hat", **"eth"**, **"ent"**, **"nth"**, **"for"**, **"his"**,
"thi", **"ter"**, **"int"**, **"dth"**, **"you"**, **"all"**,
"hes", **"ion"**, **"ith"**, **"oth"**, **"est"**, **"tth"**,
"oft", **"ver"**, **"sth"**, **"ers"**, **"fth"**, **"rea"**.

2.2. Криптоанализ аффинного шифра

В качестве простой иллюстрации использования статистического подхода рассмотрим аффинный шифр. Допустим, что получен следующий шифртекст:

УЬКЮАУХИЪЙИЯМЦЖЩИХЖУЪУЫИАБИЮЯУЖЩУЯБ

ПАБЗОАЙИЯБМЖУЪЭОТИНТГЗЩБЖЯУМБМЯИНТ

В приводимой ниже таблице дан частотный анализ шифртекста.

Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
А	4	И	8	Р	0	Ш	0
Б	6	Й	2	С	0	Щ	3
В	0	К	1	Т	3	Ъ	3
Г	1	Л	0	У	8	Ы	1
Д	0	М	4	Ф	0	Ь	1
Е	0	Н	2	Х	2	Э	1
Ж	5	О	2	Ц	1	Ю	2
З	2	П	1	Ч	0	Я	6

Таблица 3,

частотный анализ, аффинный шифр

Наиболее часто встречаются буквы **"И"**, **"У"** (по 8 раз), **"Б"**, **"Я"** (по 6 раз), **"Ж"** (5 раз), **"А"**, **"М"** (4 раза). В качестве первой попытки предположим, что буква **"И"** является образом буквы **"о"**, а буква **"У"** является образом буквы **"е"**. Иначе говоря, функция d_K должна переводить букву

"о" в букву **"и"**, а букву **"у"** — в букву **"е"**. В терминах кольца $\mathbb{Z}_{32}$ это предположение выглядит так:

$$d_K(8)=14,\ d_K(19)=5. \qquad (*)$$

В аффинном шифре функции шифрования и дешифрования имеют одинаковый вид:

$$e_K(x)=ax+b,\quad x\in\mathbb{Z}_{32};\quad d_K(y)=\alpha x+\beta,\quad y\in\mathbb{Z}_{32},$$

где a, b, α, $\beta\in\mathbb{Z}_{32}$, $(a,32)=1$, все операции выполняются в $\mathbb{Z}_{32}$, элементы α, β однозначно находятся по a и b, причем необходимо выполняется условие $(\alpha,32)=1$.

Функцию дешифрования будем искать в указанном виде, учитывая соотношения $(*)$, которые дают систему двух линейных уравнений с неизвестными α и β. При этом найденное значение c должно удовлетворять условию $(\alpha,32)=1$. Если это условие не выполняется, то наша гипотеза неверна. Если же это условие выполняется, нужно проверить что дешифрование с помощью данного отображения дает осмысленный текст. Если это так, мы расшифровали данный текст, в противном случае следует изменить гипотезы.

Итак, условия $(*)$ дают следующую систему линейных уравнений:

$$\begin{cases} 8\alpha + \beta = 14, \\ 19\alpha + \beta = 5. \end{cases}$$

Решая систему, получаем, что $\alpha=5$, $\beta=6$. Условие $(\alpha,32)=1$ выполняется. Проводя дешифрование с помощью найденной функции, получаем следующий открытый текст:

етшьжепоиуобвфдгопдеиеножлоьбедгебл

сжлймжуоблвдеичмаозахйглдбевлвбоза

Этот текст не является осмысленным. Поэтому наша исходная гипотеза неверна.

Теперь сделаем еще одну попытку. Предположим, что буква **"и"** является образом буквы **"е"**, а буква **"у"** является образом буквы **"о"**. В терминах кольца $\mathbb{Z}_{32}$ эти условия дают следующие соотношения для функции d_K:

$$d_K(8)=5, \quad d_K(19)=14. \qquad (*)$$

Система линейных уравнений для коэффициентов линейной функции d_K принимает вид:

$$\begin{cases} 8\alpha + \beta = 5, \\ 19\alpha + \beta = 14. \end{cases}$$

Находим решение $\alpha=27$, $\beta=13$. Теперь с помощью функции d_K находим открытый текст:

обычноделаетсяпредположениечтопротивник

знаетиспользуемуюкриптосистему

Этот текст является осмысленным, наша гипотеза верна. Остается найти ключ шифрования. Читателю предоставляется убедиться в том, что отображение шифрования имеет вид: $e_K(x)=19x+9$, и это отображение действительно переводит данный открытый текст в приведенный выше шифртекст.

2.3. Криптоанализ шифра подстановки

Рассмотрим теперь более сложный случай, шифр подстановки. Покажем, как проводится криптоанализ на конкретном примере.

Предположим, что рассматривается русский алфавит, состоящий из 32 букв, и с помощью шифра подстановки получен следующий шифртекст:

ЪЗПАМКАОМЕРЫМЗВАРЪАЪЗБЕЪАЮЪЗЯФЗЩИОЗСЕМЗЙ

ДЕЛЗЩТФЩКАМКБАФИЙГЕМШАФЗКАПЪЕЬРЕФЕШЕЩМТР

ЕФЕШАВТКЕМШАФАЪАСЖФЕТЫМТЩМЗОТБТЩМОЗШЗЭУТ

АМЖЩЙПАФАМЪТРЩБФАОЕХЕРДЕЩМЕЙЪЪЕХЗСЖКЗФТЛ

ЗЩТМИХЗЩЕСЕЬЩКАМКДОЕПАРЙДЕШЕХОАКЗЭПМЕШАФ

ЕХШАЩИСЖФЕЪАМЕФИБЕКЩБФАОЕХАРЪЕЛТАТХЪТГШЕ

ЩТГДЕОСЕЙФТЩИПМЕТГНШЗОТММЕБЕРЕЪТКЩАЯУАЪЗ

ХЖКЗФТЫФАБМОТПБНПНЛНЪБЕЬ

В приводимой ниже таблице дан частотный анализ шифртекста.

Буква	Частота	Буква	Частота
Е	38	Й	6
А	30	С	6
М	22	Д	5
Т	21	Ж	5
З	20	Г	4
Ф	18	Л	4
Щ	17	Н	4
Ъ	16	Ы	3
К	12	Ь	3
О	11	В	2
Б	10	У	2

Буква	Частота	Буква	Частота
Ш	10	Э	2
Р	9	Ю	1
П	8	Я	1
Х	8	Ц	0
И	6	Ч	0

Таблица 4,

частотный анализ, шифр подстановки

Буква **"Е"** встречается в шифртексте 38 раз, а буква **"А"** — 30 раз, что значительно чаще, чем любая из остальных букв. Предположим, что $d_K(\text{"Е"}) = \text{"о"}$, $d_K(\text{"А"}) = \text{"е"}$. Кроме этих букв, более 15 раз в шифртексте появляются буквы **"М"**, **"Т"**, **"З"**, **"Ф"**, **"Щ"**, **"Ъ"**. Можно предположить, что им соответствуют в открытом тексте наиболее часто встречающиеся русские буквы (кроме уже использованных **"о"** и **"е"**), то есть буквы **"а"**, **"и"**, **"н"**, **"т"**, **"с"**, **"л"**, возможно, в другом порядке, так как частоты появления указанных букв варьируются недостаточно.

Замечание. Поскольку текст содержит мало букв, здесь возможны отклонения от ожидаемого распределения. Более того, такой же факт может иметь место даже при анализе текстов большого объема, что связано с особенностями специального текста или стиля автора. Например, в книгах по криптографии часто используются слова **"криптография"**, **"шифр"**. Вследствие этого может увеличиться доля букв **"ф"**. В тексте романа М.А. Булгакова «Мастер и Маргарита» три наиболее часто встречающиеся буквы в порядке убывания их частот — это **"о"**, **"а"**, **"е"** с частотами приблизительно 65, 51 и 48 тысяч (а не **"о"**, **"е"**, **"а"**).

Вернемся к анализу шифртекста. Рассмотрим содержащиеся в нем биграммы, содержащие букву **"Е"**, то есть биграммы вида **"-Е"** и **"Е-"**.

Анализ текста дает, что наиболее часто встречаются следующие биграммы: **"МЕ"** (6 раз), **"ЕХ"**, **"ФЕ"** (по 5 раз), **"БЕ"**, **"ДЕ"**, **"ЕШ"** (по 4 раза), **"ЕМ"**, **"ЕР"**, **"ЕФ"**, **"ЕЩ"**, **"ЕЪ"**, **"ЕЬ"**, **"ОЕ"**, **"РЕ"**, **"СЕ"**, **"ШЕ"**, **"ЪЕ"** (по 3 раза). Оставим здесь биграммы, где, кроме буквы **"Е"**, стоит одна из выделенных выше букв **"М"**, **"Т"**, **"З"**, **"Ф"**, **"Щ"**, **"Ъ"**. Получаем биграммы **"МЕ"** (6 раз), **"ФЕ"** (5 раз), **"ЕМ"**, **"ЕФ"**, **"ЕЩ"**, **"ЕЪ"**, **"ЪЕ"** (по 3 раза). Наиболее часто встречающаяся в русском языке биграмма вида "-о" — это **"то"**. Поэтому правдоподобным является предположение, что $d_K(\text{"М"}) = \text{"т"}$. Заметим, что из оставшихся биграмм восемь раз встречается биграмма **"ЕФ"** или **"ФЕ"**, и шесть раз встречается биграмма **"ЕЪ"** или **"ЪЕ"**. Им, в соответствии с нашим предположением, должны в открытом тексте соответствовать биграммы "о-" или "-о" , содержащие *одну и ту же букву,* обозначенную черточкой. Приведем часть таблицы вероятностей появления биграмм, содержащих букву **"о"**. Таблица дана для биграмм с *наибольшей суммарной вероятностью*.

"-о"	Вероятность	"о-"	Вероятность	Сумма вероятностей
то	0.014834	от	0.008732	0.023566
но	0.012131	он	0.009716	0.021847
во	0.007492	ов	0.010135	0.017627
ро	0.008528	ор	0.007092	0.015620
по	0.011059	оп	0.004064	0.015123
ло	0.007188	ол	0.007532	0.014720
го	0.008041	ог	0.005787	0.013828
ко	0.009805	ок	0.003739	0.013544
со	0.003603	ос	0.009659	0.013262
мо	0.005267	ом	0.007073	0.012340

"-о"	Вероятность	"о-"	Вероятность	Сумма вероятностей
до	0.004550	од	0.006465	0.011015

Таблица 5,

вероятности биграмм "о-" **или** "-о"

Удалим здесь биграммы, соответствующие уже использованным по предположению буквам открытого текста (**"е"**, **"т"**), и биграммы, которые, кроме буквы **"о"** содержат букву, отличную от приведенных выше букв открытого текста **"а"**, **"и"**, **"н"**, **"т"**, **"с"**, **"л"**.

"-о"	Вероятность	"о-"	Вероятность	Сумма вероятностей
но	0.012131	он	0.009716	0.021847
ло	0.007188	ол	0.007532	0.014720
со	0.003603	ос	0.009659	0.013262

Таблица 6

Отсюда видно, что буквы **"Ф"** и **"Ъ"** могут быть дешифрованы как одна из следующих букв: **"н"**, **"л"**, **"с"**. Заметим, что биграммы **"ФЕ"** и **"ЕФ"** входят с частотами (5+3), отличающимися менее, чем в два раза, а биграммы **"ЪЕ"** и **"ЕЪ"** — с одинаковыми частотами (3+3). Учитывая существенную разницу в распределении вероятностей для **"со"** и **"ос"**, исключим букву **"с"** из рассмотрения, то есть будем предполагать, что буквы **"Ф"** и **"Ъ"** дешифруются как **"н"**или **"л"**. Для того, чтобы выбрать нужный вариант, перейдем к анализу *триграмм*, имеющихся в тексте.

В шифртексте триграммы "**АМК**" и "**ШАФ**" встречаются по три раза, а каждая из триграмм **"АОЕ"**, **"АРЪ"**, **"АФА"**, **"АЪЗ"**, **"БФА"**, **"ЕМШ"**, **"ЕФЕ"**, **"ЕША"**, **"ЕШЕ"**, **"ЕЩМ"**, **"ЕЪА"**, **"ЖКЗ"**, **"ЖФЕ"**, **"ЗОТ"**, **"ЗФТ"**,

"ЗЩТ", **"ЙДЕ"**, **"КАМ"**, **"КЗФ"**, **"ЛЗЩ"**, **"МША"**, **"ОЕХ"**, **"ПМЕ"**, **"РЕФ"**, **"СЖФ"**, **"ТЩМ"**, **"ФАО"**, **"ФЕШ"**, **"ШЕЩ"**, **"ЩБФ"**, **"ЩКА"** — по два раза. Удалим отсюда все триграммы, кроме состоящих из букв **"Е"**, **"А"**, **"М"**, **"Т"**, **"З"**, **"Ф"**, **"Щ"**, **"Ъ"**. Мы получаем триграммы **"АФА"**, **"АЪЗ"**, **"ЕФЕ"**, **"ЕЩМ"**, **"ЕЪА"**, **"ЗФТ"**, **"ЗЩТ"**, **"ТЩМ"**, встречающиеся по два раза.

Триграмма **"ЕФЕ"** встречается два раза, а триграмма "**ЕЪЕ**" не встречается. В открытом тексте, в соответствии с нашим предположением, им соответствуют триграммы **"оно"** или **"оло"**. Приведем вероятности появления триграмм вида **"о-о"**.

Триграмма	Вероятность	Триграмма	Вероятность
ото	0.002343	обо	0.000730
оро	0.001967	осо	0.000680
ово	0.001695	оно	0.000665
оло	0.001445	охо	0.000464
опо	0.001312	ойо	0.000209
око	0.000951	ошо	0.000132
одо	0.000919	оео	0.000118
омо	0.000886	озо	0.000066

Таблица 7,

вероятности триграмм "о-о"

Как видно из таблицы, триграмма **"оло"** примерно в два раза более вероятна, чем **"оно"**. Можно сделать предположение, что $d_K(\text{"Ф"}) = \text{"л"}$, и тогда $d_K(\text{"Ъ"}) = \text{"н"}$.

Триграмма "**ШАФ**" встречается три раза и, в силу наших гипотез, расшифровывается, как "**-ел**" с неизвестной пока буквой. Приведем таблице вероятностей триграмм вида "**-ел**".

Триграмма	Вероятность	Триграмма	Вероятность
тел	0.001754	мел	0.000238
дел	0.001458	нел	0.000225
чел	0.000426	бел	0.000183
рел	0.000421	цел	0.000172
вел	0.000410	пел	0.000140
шел	0.000375	зел	0.000074
жел	0.000323	лел	0.000067
сел	0.000243	иел	0.000057

Таблица 8,

вероятности триграмм "-ел"

Буква **"т"** нами уже использована. Будем предполагать, что $d_K(\text{"Ш"}) = \text{"д"}$.

Посмотрим, что получается при дешифровке на данном этапе:

н--ет-е-то--т--е-нен--оне-н--л------от--

ЪЗПАМКАОМЕРЫМЗВАРЪАЪЗБЕЪАЮЪЗЯФЗЩИОЗСЕМЗЙ

-о----л--ет--ел---отдел--е-но--олодо-т--

ДЕЛЗЩТФЩКАМКБАФИЙГЕМШАФЗКАПЪЕЬРЕФЕШЕЩМТР

олоде---отделене--ло--т--т------т--д----

ЕФЕШАВТКЕМШАФАЪАСЖФЕТЫМТЩМЗОТБТЩМОЗШЗЭУТ

ет----елетн----ле-о-о--о-то-нно------л--

АМЖЩЙПАФАМЪТРЩБФАОЕХЕРДЕЩМЕЙЪЪЕХЗСЖКЗФТЛ

---т----о-о---ет---о-е---одо--е----тодел

ЗЩТМИХЗЩЕСЕЬЩКАМКДОЕПАРЙДЕШЕХОАКЗЭПМЕШАФ

о-де----лонетол--о---ле-о-е-но--е--н--до

ЕХШАЩИСЖФЕЪАМЕФИБЕКЩБФАОЕХАРЪЕЛТАТХЪТГШЕ


----о--о-л----то---д---тто-о-он---ее-ен-

ЩТГДЕОСЕЙФТЩИПМЕТГНШЗОТММЕБЕРЕЪТКЩАААУАЪЗ

----л--ле-т---------н-о-

ХЖКЗФТЫФАБМОТПБНПНЛНЪБЕЬ

Из оставшихся букв шифртекста наибольшие частоты имеют **"Т"** (21 раз) и **"З"** (20 раз). Рассматривая приведенную выше частичную дешифровку, видим, что в тех случаях, когда для прообраза каждой из этих букв соседняя буква уже выбрана, эта соседняя буква является согласной. Поэтому весьма правдоподобно, что d_K("Т") и d_K("З") — гласные буквы. Из гласных букв, для которых пока не найдено соответствие, наибольшую вероятность имеют **"и"** и **"а"** Будем предполагать, что одна из букв **"Т"**, **"З"** дешифруется, как **"и"**, а другая, как **"а"**.

Следующая по частоте буква шифртекста — это **"Щ"**. Биграмма **"ЩМ"** встречается в шифртекста 4 раза и дешифруется как **"-т"**. Среди биграмм вида **"-т"** наибольшую вероятность имеет биграмма **"ст"** (см. таблицу).

Биграмма	Вероятность	Биграмма	Вероятность
ст	0.013005	ят	0.002156
от	0.008732	нт	0.001314
ет	0.007371	кт	0.001239
ат	0.006374	ыт	0.001169
ит	0.005709	рт	0.000936
чт	0.003494	ют	0.000834
эт	0.002676	вт	0.000794
ут	0.002171	йт	0.000752

Таблица 9,

вероятности биграмм "-т"

Поэтому будем предполагать, что $d_K(\text{"Щ"}) = \text{"с"}$. Из двух вариантов дешифровки букв **"Т"**, **"З"** попробуем следующий: $d_K(\text{"Т"}) = \text{"и"}$, $d_K(\text{"З"}) = \text{"а"}$ и попытаемся дешифровать текст при данных условиях:

на-ет-е-то--та-е-нена-оне-на-лас--а-ота-
ЪЗПАМКАОМЕРЫМЗВАРЪАЪЗБЕЪАЮЪЗЯФЗЩИОЗСЕМЗЙ
-о-асилс-ет--ел---отдела-е-но--олодости-
ДЕЛЗЩТФЩКАМКБАФИЙГЕМШАФЗКАПЪЕЬРЕФЕШЕЩМТР
олоде-и-отделене--лои-тиста-и-ист-ада--и
ЕФЕШАВТКЕМШАФАЪАСЖФЕТЫМТЩМЗОТБТЩМОЗШЗЭУТ
ет-с--елетни-с-ле-о-о--осто-нно-а---али-
АМЖЩЙПАФАМЪТРЩБФАОЕХЕРДЕЩМЕЙЪЪЕХЗСЖКЗФТЛ
асит--асо-о-с-ет---о-е---одо--е-а--тодел
ЗЩТМИХЗЩЕСЕЬЩКАМКДОЕПАРЙДЕШЕХОАКЗЭПМЕШАФ
о-дес---лонетол--о-с-ле-о-е-но-иеи-ни-до
ЕХШАЩИСЖФЕЪАМЕФИБЕКЩБФАОЕХАРЪЕЛТАТХЪТГШЕ
си--о--о-лис--тои--да-итто-о-они-сее-ена
ЩТГДЕОСЕЙФТЩИПМЕТГНШЗОТММЕБЕРЕЪТКЩААУАЪЗ
---али-ле-т-и-------н-ой
ХЖКЗФТЫФАБМОТПБНПНЛНЪБЕЬ

Будем считать, что

1) фрагмент **"-олодости"** дешифруется, как **"молодости"**, то есть $d_K(\text{"Р"}) = \text{"м"}$;

2) фрагмент **"нетол--о"** — как **"нетолько"**, то есть $d_K(\text{"И"}) = \text{"ь"}$;, то есть $d_K(\text{"Б"}) = \text{"к"}$.

на-ет-е-том-та-емненаконе-на-лась-а-ота-
ЪЗПАМКАОМЕРЫМЗВАРЪАЪЗБЕЪАЮЪЗЯФЗЩИОЗСЕМЗЙ
-о-асилс-ет-кель--отдела-е-но-молодостим
ДЕЛЗЩТФЩКАМКБАФИЙГЕМШАФЗКАПЪЕЬРЕФЕШЕЩМТР


олоде-и-отделене--лои-тиста-икист-ада--и

ЕФЕШАВТКЕМШАФАЪАСЖФЕТЫМТЩМЗОТБТЩМОЗШЗЭУТ

ет-с--елетнимскле-о-ом-осто-нно-а---али-

АМЖЩЙПАФАМЪТРЩБФАОЕХЕРДЕЩМЕЙЪЪЕХЗСЖКЗФТЛ

асить-асо-о-с-ет---о-ем--одо--е-а--тодел

ЗЩТМИХЗЩЕСЕЬЩКАМКДОЕПАРЙДЕШЕХОАКЗЭПМЕШАФ

о-десь--лонетолько-скле-о-емно-иеи-ни-до

ЕХШАЩИСЖФЕЪАМЕФИБЕКЩБФАОЕХАРЪЕЛТАТХЪТГШЕ

си--о--о-лись-тои--да-иттокомони-сее-ена

ЩТГДЕОСЕЙФТЩИПМЕТГНШЗОТММЕБЕРЕЪТКЩАААУАЪЗ

---али-лект-и-к-----нко-

ХЖКЗФТЫФАБМОТПБНПНЛНЪБЕЬ

Строка **"мненаконе-"** (первая строка открытого текста) может быть уточнена, как **"мненаконец"**, то есть $d_K(\text{"Ю"}) = \text{"ц"}$, строка **"молоде-и"** (вторая и третья строки открытого текста) может быть уточнена, как **"молодежи"**, то есть $d_K(\text{"В"}) = \text{"ж"}$, строка **"скле-о-ом"** (четвертая строка открытого текста) может быть расшифрована, как **"скле-о-ом"**, то есть $d_K(\text{"О"}) = \text{"р"}$, $d_K(\text{"Х"}) = \text{"з"}$. Теперь дешифрование дает:

на-ет-ертом-тажемненаконецна-ласьра-ота-

ЪЗПАМКАОМЕРЫМЗВАРЪАЪЗБЕЪАЮЪЗЯФЗЩИОЗСЕМЗЙ

-о-асилс-ет-кель--отдела-е-но-молодостим

ДЕЛЗЩТФЩКАМКБАФИЙГЕМШАФЗКАПЪЕЬРЕФЕШЕЩМТР

олодежи-отделене--лои-тистарикистрада--и

ЕФЕШАВТКЕМШАФАЪАСЖФЕТЫМТЩМЗОТБТЩМОЗШЗЭУТ

ет-с--елетнимсклерозом-осто-ннозa---али-

АМЖЩЙПАФАМЪТРЩБФАОЕХЕРДЕЩМЕЙЪЪЕХЗСЖКЗФТЛ

аситьзасо-о-с-ет--ро-ем--одозре-а--тодел

ЗЩТМИХЗЩЕСЕЬЩКАМКДОЕПАРЙДЕШЕХОАКЗЭПМЕШАФ


оздесь--лонетолько-склероземно-иеизни-до

ЕХШАЩИСЖФЕЪАМЕФИБЕКЩБФАОЕХАРЪЕЛТАТХЪТГШЕ

си--ор-о-лись-тои--дариттокомони-сее-ена

ЩТГДЕОСЕЙФТЩИПМЕТГНШЗОТММЕБЕРЕЪТКЩАААУАЪЗ

з--али-лектри-к-----нко-

ХЖКЗФТЫФАБМОТПБНПНЛНЪБЕЬ

Теперь возможны следующие уточнения.

В первой строке

"-таже" —**"этаже"**, то есть $d_K(\text{"Ы"}) = \text{"э"}$;

"-ет-ертом" —**"четвертом"**, $d_K(\text{"П"}) = \text{"ч"}$, $d_K(\text{"К"}) = \text{"в"}$; **"на-лась"** — **"нашлась"**, $d_K(\text{"Я"}) = \text{"ш"}$;

"ра-ота" — **"работа"**, $d_K(\text{"С"}) = \text{"б"}$.

В четвертой строке:

"т-с--елетним", учитывая, что $d_K(\text{"П"}) = \text{"ч"}$, переходит в **"т-с-челетним"**, и уточняется до **"тысячелетним"**, то есть $d_K(\text{"Ж"}) = \text{"ы"}$, $d_K(\text{"Й"}) = \text{"я"}$;

"-одозре-а-" с учетом того, что $d_K(\text{"К"}) = \text{"в"}$, уточняется до **"-одозрева-"**, и тогда первая буква должна быть **"п"**, то есть $d_K(\text{"Д"}) = \text{"п"}$.

Теперь дешифрованный текст выглядит так:

начетвертомэтажемненаконецнашласьработая

ЪЗПАМКАОМЕРЫМЗВАРЪАЪЗБЕЪАЮЪЗЯФЗЩИОЗСЕМЗЙ

по-асилсветвкелья-отделавечно-молодостим

ДЕЛЗЩТФЩКАМКБАФИЙГЕМШАФЗКАПЪЕЬРЕФЕШЕЩМТР

олодеживотделенебылоиэтистарикистрада--и

ЕФЕШАВТКЕМШАФАЪАСЖФЕТЫМТЩМЗОТБТЩМОЗШЗЭУТ

етысячелетнимсклерозомпостояннозабывали-

АМЖЩЙПАФАМЪТРЩБФАОЕХЕРДЕЩМЕЙЪЪЕХЗСЖКЗФТЛ

аситьзасобо-светвпрочемяподозрева-чтодел

ЗЩТМИХЗЩЕСЕЬЩКАМКДОЕПАРЙДЕШЕХОАКЗЭПМЕШАФ

оздесьбылонетольковсклероземно-иеизни-до

ЕХШАЩИСЖФЕЪАМЕФИБЕКЩБФАОЕХАРЪЕЛТАТХЪТГШЕ

си-порбоялисьчтои--дариттокомонивсее-ена

ЩТГДЕОСЕЙФТЩИПМЕТГНШЗОТММЕБЕРЕЪТКЩАЛУАЪЗ

зывалиэлектричк-ч---нко-

ХЖКЗФТЫФАБМОТПБНПНЛНЪБЕЬ

Теперь легко уточняются остальные буквы (по смыслу текста и с учетом тех букв, которые до сих не расшифрованы). Окончательно получаем следующий шифртекст:

начетвертомэтажемненаконецнашласьработая

погасилсветвкельяхотделавечноймолодостим

олодеживотделенебылоиэтистарикистрадающи

етысячелетнимсклерозомпостояннозабывалиг

аситьзасобойсветвпрочемяподозреваючтодел

оздесьбылонетольковсклероземногиеизнихдо

сихпорбоялисьчтоихудариттокомонивсеещена

зывалиэлектричкучугункой

После расстановки пробелов и знаков препинания, находим исходный открытый текст:

На четвертом этаже мне, наконец, нашлась работа: я погасил свет в кельях отдела Вечной Молодости. Молодежи в отделе не было, и эти старики, страдающие тысячелетним склерозом, постоянно забывали гасить за собой свет. Впрочем, я подозреваю, что дело здесь было не только в склерозе. Многие из них до сих пор

боялись, что их ударит током. Они все еще называли электричку чугункой.[1]

[1] А.Н. Стругацкий, Б.Н. Стругацкий. *Понедельник начинается в субботу.*

2.4. Криптоанализ шифра Виженера

В этом разделе будут описаны некоторые методы криптоанализа шифра Виженéра.

В случае рассматриваемого шифра, прежде всего, нужно найти длину ключевого слова, которую мы обозначим через l. Приведем два метода, которые могут быть использованы для этого. Первый из них — это *тест Казиски,* а второй — метод *индексов совпадения.*

Тест Казиски был предложен Ф. Казиски в 1863 году. Он основан на следующих соображениях: если два одинаковых отрезка открытого текста получаются один из другого сдвигом на величину, кратную длине ключевого слова, то они при шифровании перейдут в одинаковые отрезки шифртекста. Эти аргументы используются следующим образом: если в шифртексте имеются два фрагмента длины три или больше, то весьма вероятно, что они соответствуют одинаковым отрезкам открытого текста.

Тест Казиски применяется так. Ищем в шифртексте пары одинаковых отрезков длины три или больше. Находим расстояние между стартовыми позициями этих отрезков. Если мы найдем несколько таких расстояний d_1, d_2,… , то можно предположить, что искомое число l является делителем каждого из этих чисел и, следовательно, делителем их наибольшего общего делителя.

Дальнейшие аргументы для нахождения числа l могут быть получены с помощью *индексов совпадения*. Это понятие было введено В. Фридманом в 1920 году.

ОПРЕДЕЛЕНИЕ. *Пусть* $\mathbf{x}$ *— строка, составленная из букв некоторого алфавита. Индексом совпадения строки* $\mathbf{x}$ *называется вероятность того,*

что две случайно выбранных из этой строки буквы являются одинаковыми.

Индекс совпадения строки $\mathbf{x}$ будем обозначать через $I(\mathbf{x})$.

Будем предполагать, что рассматриваемый алфавит содержит m букв, пронумерованных числами $0, 1, \ldots, m-1$. Рассмотрим строку $\mathbf{x}$, содержащую n букв. Мы можем выбрать две буквы из этой строки,

$$C_n^2 = \frac{n(n-1)}{2}$$

способами. Предположим, что буква с номером i $(0 \le i \le m-1)$ встречается в этой строке f_i раз (напомним, что значение f_i называется частотой или, точнее, абсолютной частотой рассматриваемой буквы). Для произвольного $i(=0,1,\ldots,m-1)$ имеется $C_{f_i}^2$ способов выбрать одинаковые буквы с номером i. Отсюда получаем, что

$$I(\mathbf{x}) = \frac{\sum_{i=0}^{m-1} f_i(f_i-1)}{n(n-1)}.$$

Обозначим через p_0, $p_1,\ldots,p_{m-1}$ *вероятности* появления букв алфавита в этой строке, то есть *относительные частоты* f_0/n, f_1/n, …, f_{m-1}/n. Тогда при *достаточно большом значении* n, имеет место *приближенная* формула

$$I_c(\mathbf{x}) \approx \sum_{i=0}^{m-1} p_i^2,$$

так как вероятность дважды выбрать букву с номером 0 *приблизительно* равна p_0^2, букву с номером 1 — p_1^2, и так далее.

Предположим теперь, что строка составлена из букв естественного языка, например, русского или английского. Пользуясь таблицами, приведенными выше, получаем следующие значения индекса совпадения для

строки большой длины, являющейся : русский алфавит —**0.0553**, английский алфавит —**0.0644**. Те же значения будут получены и *для любого шифртекста,* полученного с помощью произвольного моноалфавитного шифра. Действительно, в этом случае вероятности отдельных букв поменяются местами, но *сумма* этих вероятностей останется неизменной.

Предположим, что дан шифртекст $\mathbf{y} = y_1 y_2 \ldots y_n$, полученный с помощью шифра Виженера. Сделаем предположение, что длина ключевого слова равна l. Введем в рассмотрение буквенный массив, состоящий из l строк и n/l столбцов. Запишем символы данного шифртекста по столбцам в этот массив. Строки этого массива обозначим через $\mathbf{y}_1$, $\mathbf{y}_2, \ldots, \mathbf{y}_l$. Если мы правильно нашли значение l, то каждая из строк $\mathbf{y}_1$, $\mathbf{y}_2, \ldots, \mathbf{y}_l$ получена из соответствующих подстрок исходного открытого текста с помощью шифра сдвига. Тогда значения $I(\mathbf{y}_i)$ $(1 \le i \le l)$ должны быть приближенно равны значению индекса совпадения для соответствующего языка (то есть **0.0553** для русского языка и **0.0644** для английского). Если мы неверно нашли значение l (точнее, если настоящее значение длины ключевого слова не является делителем числа l), то найденные подстроки уже будут иметь более случайную структуру, поскольку они получаются с помощью шифра сдвига с разными ключами. Заметим, что для полностью случайной строки в случае алфавита из m символов

$$I(\mathbf{x}) \approx m\left(\frac{1}{m}\right)^2 = \frac{1}{m}.$$

В случае русского языка это дает **0.03125**, в случае английского языка — **0.03856**. Для двух рассматриваемых языков это существенно отличается от приведенных выше значений и может позволить определить правильную длину ключевого слова (или подтвердить догадку, сделанную с помощью теста Казиски).

После определения длины ключевого слова нужно, разумеется, найти само это слово.

ОПРЕДЕЛЕНИЕ. *Пусть* $\mathbf{x}$, $\mathbf{y}$ *— строка, составленные из букв некоторого алфавита. Взаимным индексом совпадения этих строк называется вероятность того, что буква, случайно выбранная из первой строки, совпадает с буквой, случайно выбранной из второй строки.*

Взаимный индекс совпадения двух строк $\mathbf{x}$, $\mathbf{y}$ будем обозначать через $MI(\mathbf{x},\mathbf{y})$ ("*Mutual Index*"). Рассмотрим алфавит, состоящий из m букв. Пусть

$$\mathbf{x} = x_1 x_2 \ldots x_n, \quad \mathbf{y} = y_1 y_2 \ldots y_{n'},$$

p_0, $p_1, \ldots, p_{m-1}$ — вероятности того, что случайно выбранная из первой строки буква является соответственно первой, второй, …, m-й буквой алфавита, q_0, $q_1, \ldots, q_{m-1}$ — аналогичные характеристики для второй строки. Тогда, очевидно,

$$MI(\mathbf{x},\mathbf{y}) = \sum_{i=0}^{m-1} p_i q_i.$$

Обозначим через f_0, f_1, ,…, f_{m-1} частоты соответствующих букв алфавита в первой строке, а через f'_0, f'_1, ,…, f'_{m-1} — соответствующие характеристики для второй строки. Тогда

$$MI(\mathbf{x},\mathbf{y}) = \frac{\sum_{i=0}^{m-1} f_i f'_i}{nn'}.$$

Возьмем произвольный шифр подстановки. Это означает, что выбрана произвольная подстановка $\varphi \in \mathfrak{S}_m$, рассматриваемая на множестве $\mathbb{Z}_m$, и буква алфавита с номером i заменяется буквой с номером $\varphi(i)$. Предположим, что строки $\mathbf{x}$ и $\mathbf{y}$ зашифрованы с помощью этого шифра. Пусть $\tilde{\mathbf{x}}$, $\tilde{\mathbf{y}}$ — соответствующие строки шифртекста. Если, как и выше, p_0, $p_1, \ldots,$

p_{m-1} — вероятности выбора соответствующих букв алфавита из строки $\mathbf{x}$, q_0, $q_1,\ldots,q_{m-1}$ — аналогичные характеристики для строки $\mathbf{y}$. Для строки $\tilde{\mathbf{x}}$ эти вероятности равны $p_{\varphi^{-1}(0)}$, $p_{\varphi^{-1}(1)},\ldots,p_{\varphi^{-1}(m-1)}$. Тогда

$$MI(\tilde{\mathbf{x}},\tilde{\mathbf{y}}) = \sum_{i=0}^{m-1} p_{\varphi^{-1}(i)} q_{\varphi^{-1}(i)} = \sum_{i=0}^{m-1} p_i q_i = MI(\mathbf{x},\mathbf{y}),$$

поскольку выписанные суммы отличаются только порядком следования слагаемых. Аналогично доказывается, что $I(\tilde{\mathbf{x}}) = I(\mathbf{x})$.

Мы получили важный факт: *индекс совпадения строки и взаимный индекс совпадения двух строк не меняются после шифровании этих строк произвольным шифром подстановки.*

Вернемся к анализу шифра Виженера. Пусть $K = (k_1, k_2,\ldots,k_l)$ — ключевое слово. Попробуем оценить величину $MI(\mathbf{y}_i,\mathbf{y}_j)$. Выберем случайным образом букву из строки $\mathbf{y}_i$ и букву из строки $\mathbf{y}_j$. Учтем, что каждая рассматриваемых строк шифруется с помощью шифра сдвига, первая — с ключом k_i, вторая — с ключом k_j. Вероятность того, что первая (вторая) из этих букв совпадает с первой буквой алфавита (нулем в $\mathbb{Z}_m$), равна p_{-k_i} (p_{-k_j}).Следовательно, вероятность того, что обе буквы совпадают с первой буквой алфавита, равна $p_{-k_i} p_{-k_j}$.

ЗАМЕЧАНИЕ. Здесь и далее в индексах операции выполняются в кольце $\mathbb{Z}_m$. Все равенства являются приближенными, поскольку вероятности появления букв в данных строках лишь приближенно равны среднестатистическим величинам.

Аналогично получаем: вероятность того, что обе буквы совпадают с второй буквой алфавита (элементом 1 в $\mathbb{Z}_m$), равна $p_{1-k_i} p_{1-k_j}$. Следовательно,

$$MI(\mathbf{y}_i, \mathbf{y}_j) \approx \sum_{h=0}^{m-1} p_{h-k_i} p_{h-k_j} = \sum_{h=0}^{m-1} p_h p_{r+k_i-k_j}.$$

Заметим, что правая часть этого выражения зависит только от *разности* $k_i - k_j$, которую будем называть *относительным сдвигом* строк $\mathbf{y}_i$ и $\mathbf{y}_j$.

Учтем следующую очевидную формулу:

$$\sum_{h=0}^{m-1} p_h p_{h+\alpha} = \sum_{h=0}^{m-1} p_h p_{h-\alpha}, \quad \alpha \in \mathbb{Z}_m,$$

то есть относительный сдвиг на величину α дает то же значение величины MI, что и сдвиг на величину $m - \alpha$. Это означает, что в случае алфавита из m букв, достаточно найти значения MI для значений $\alpha = 0, 1, \ldots, [m/2]$. Приведем эти значения для русского и английского языков.

Относительный сдвиг	Взаимный индекс
0	0.0553
1	0.0366
2	0.0345
3	0.0400
4	0.0340
5	0.0360
6	0.0326
7	0.0241
8	0.0287
9	0.0317
10	0.0265
11	0.0251
12	0.0244
13	0.0291

Относительный сдвиг	Взаимный индекс
14	0.0322
15	0.0244
16	0.0249

Таблица 10.

Взаимный индекс совпадения (русский язык)

Относительный сдвиг	Взаимный индекс
0	0.0644
1	0.0394
2	0.0319
3	0.0345
4	0.0436
5	0.0332
6	0.0363
7	0.0389
8	0.0338
9	0.0342
10	0.0378
11	0.0440
12	0.0387
13	0.0428

Таблица 11.

Взаимный индекс совпадения (английский язык)

Отметим следующее. Если относительный сдвиг в случае русского (английского) языка ненулевой, то значения взаимного индекса варьируются от **0.0241** до **0.0400** (от **0.0319** до **0.0440**), в то время как относи-

тельный индекс для нулевого относительного сдвига равен **0.0553** (соответственно **0.0644**). Это наблюдение позволяет делать правдоподобные предположения относительно разностей $\beta = K_i - K_j$.

Зафиксируем числа i, j, $1 \le i, j \le l$, $i \ne j$. Возьмем строки $\mathbf{y}_i$ и $\mathbf{y}_j$. Рассмотрим строки, получающиеся путем применения шифров сдвига со всеми возможными значениями ключа (то есть 0, 1, …, $m-1$) к строке $\mathbf{y}_j$. Обозначим получаемые строки через $\mathbf{y}_j^0$, $\mathbf{y}_j^1$, … , $\mathbf{y}_j^{m-1}$ ($m = 32$ в случае русского алфавита и $m = 26$ в случае английского алфавита). Теперь найдем соответствующие значения взаимного индекса совпадения $MI_c(\mathbf{y}_i, \mathbf{y}_j^\beta)$, $\beta = 0$, 1, … , $m-1$. При $\beta = \alpha$ взаимный индекс совпадения должен быть близким к наибольшему значению для данного языка, поскольку относительный сдвиг между $\mathbf{y}_i$ и $\mathbf{y}_j^\alpha$ равен нулю. При $\beta \ne \alpha$ рассматриваемая величина должна принимать существенно меньшие значения.

Пример. Рассмотрим шифртекст, полученный с использованием шифра Виженера:

СЮРСЕЫПЛУИДЮПЖДЭТВЙЛЧЯЭХИЪЩЭРОСШЕПКЭЭЕБТФЫКОО
ЮЮЩФЧЧЫХГАЬШУВОХХЯУВПЯУТСБРЫПВЧЫЯАНПЧОЕНЧХЩБП
КШФЖВПЫЭЙДХРШРЕАШХФЧЧЫХГОЬЮШХИЪЩЭРАГШЩЙПЮЮРЙЧ
ПФРБПЭЫЫПЗСГЕОЫДЮАСЫСШЯУЫДЕЬИЯШБШЙХВФОСАЧТЙМЕ
БРЩТЛПХЪГСБАУШАБМУДОСЯУСЕУЭУКХЭЧНЙНСТОМИСРЩТЯ
СЗУСНЭСБСОШЫЦТЕАТУСКППЪЙЛЪШЬООЫБЫЖЖЬЛГВЛФБАПК
ЮРГОУИШЧНАЬФОСИЬРЪЙСЧУОСАЫШТФХПЬЦМИЫЮЫБМЧСУОЗ
ЧЭЬНОУХШПЛЭЭЬНСВЪЫПМЧУЬМОАХСПКПЪШПМПЭТОАОВЮФБ
ПАОИНЭБЦМСОЯЬГСФЬБЗИЪЩЗФ

Прежде всего, воспользуемся тестом Казиски. Триграмма **"ИЪШ"** появляется в тексте три раза, начинаясь с букв с номерами **25**, **120** и **380**

(подчеркнуто в шифртексте). Разности между этими числами равны **95** и **260**. Наибольший общий делитель двух последних чисел равен пяти. Поэтому правдоподобной является гипотеза, что $l = 5$.

Посмотрим, дает ли подсчет индексов совпадения такой же вывод. При $l = 1$ индекс совпадения (всей строки шифртекста) равен **0.0360**.

При $l = 2$ текст разбивается на две строки

СРЕПУДПДТЙЧЭИШРСЕКЭБФКОЮФЧХАШВХЯВЯТБЫВЫАПОНХБ
КФВЫЙХШЕШФЧХОЮХЪЭАШЙЮРЧФБЭЫЗГОДАЫШУДЬЯБЙВОАТМ
БЩЛХГБУАМДСУЕЭКЭННТМСЩЯЗСЭБОЫТАУКПЙЪЬОБЖЬГЛБП
ЮГУШНЬОИРЙЧОАШФПЦИЮБЧУЗЭНУШЛЭНВЫМУМАСКЪППТАВФ
ПОНБМОЬСЬЗЪЗ

и

ЮСЫЛИЮЖЭВЛЯХЪЭОШПЭЕТЫОЮЩЧЫГЬУОХУПУСРПЧЯНЧЕЧЩП
ШЖПЭДРРАХЧЫГЬШИШРГЩПЮЙПРПЫПСЕЫЮССЯЫЕИШШХФСЧЙЕ
РТПЪСАШБУОЯСУУХЧЙСОИРТСУНССШЦЕТСПЪЛШОЫЬЖЛВФАК
РОИЧАФСЬЪСУСЫТХЬМЫЫМСОЧЬОХПЭЬСЪПЧЬОХППШМЭООЮБ
АИЭЦСЯГФБИШФ

с индексами совпадения соответственно **0.0323** и **0.0417**. При $l = 3$ индексы совпадения равны соответственно **0.0389**, **0.0337** и **0.0359**, при $l = 4$ — **0.0309**, **0.0425**, **0.0340** и **0.0373**, при $l = 5$ —**0.0635**, **0.0561**, **0.0435**, **0.0547** и **0.0526**, при $l = 6$ — **0.0332**, **0.0382**, **0.0283**, **0.0397**, **0.0322** и **0.0486**. Заметное увеличение индексов совпадения при $l = 5$ также говорит в пользу нашей гипотезы.

Теперь попробуем найти величины относительных сдвигов. Приведем таблицу 320 значений величин $MI_c(\mathbf{y}_i, \mathbf{y}_j^{\beta})$, $1 \le i < j \le 5$, $0 \le \beta \le 31$. В ней значения индекса указаны в порядке возрастания величины β от нуля до 31. В этих значениях отброшены начальные символы **0.0**. Для каждой

пары (i, j) выберем наибольшее значение индекса. Это значение подчеркнуто.

i	j	Значение $MI_c(\mathbf{y}_i, \mathbf{y}_j^{\beta})$
1	2	391 306 405 398 313 402 313 279 294 277 232 216 296 220 218 178 289 279 284 241 305 184 317 362 211 414 346 255 455 395 294 <u>630</u>
1	3	322 <u>495</u> 358 339 436 362 268 319 298 348 325 211 263 232 300 255 220 189 305 260 284 268 312 293 294 280 272 355 462 267 419 390
1	4	383 260 312 350 206 298 429 263 435 409 315 438 431 362 <u>563</u> 403 338 341 301 293 338 258 213 220 185 185 216 263 220 239 289 246
1	5	336 289 325 306 284 255 362 331 211 447 372 270 391 390 267 <u>604</u> 370 320 367 376 293 324 313 303 296 216 263 173 336 232 248 130
2	3	405 351 <u>525</u> 374 343 499 332 301 353 249 341 305 225 268 237 237 244 192 189 268 220 249 248 261 310 317 272 312 398 400 345 429
2	4	239 267 242 305 334 229 355 438 289 469 443 374 532 412 417 <u>587</u> 370 336 421 249 268 319 216 234 235 161 189 197 204 209 227 232
2	5	190 263 235 294 272 234 308 381 268 291 474 322 348 464 355 325 <u>616</u> 364 332 466 319 306 345 249 303 296 211 249 189 272 230 227
3	4	255 277 360 220 370 376 300 424 358 376 <u>506</u> 424 424 <u>459</u> 357 369 391 306 348 306 275 218 251 227 204 223 229 204 237 229 204 293

i	j	Значение $MI_c(\mathbf{y}_i, \mathbf{y}_j^{\beta})$
3	5	268 272 291 244 284 362 332 293 353 319 351 443 343 339 <u>547</u> 348 358 376 315 407 353 280 251 298 301 261 215 256 244 282 206 206
4	5	384 <u>521</u> 409 452 485 353 388 433 277 383 327 201 303 251 249 265 206 239 251 222 258 235 209 222 296 235 265 360 310 282 400 329

Таблица 12.

Значения взаимных индексов совпадения

Выпишем уравнения (в кольце $\mathbb{Z}_{32}$), связывающие неизвестные значения K_1, K_2, K_3, K_4, K_5, отвечающие наибольшим из шести подчеркнутых значений:

$$K_1 - K_2 = 31, \quad K_2 - K_5 = 16, \quad K_1 - K_5 = 15,$$
$$K_2 - K_4 = 15, \quad K_1 - K_4 = 14, \quad K_3 - K_5 = 14.$$

Эти уравнения позволяют выразить все значения K_i через K_1:

$$K_2 = K_1 + 1, \quad K_3 = K_1 + 31, \quad K_4 = K_1 + 18, \quad K_5 = K_1 + 17.$$

Таким образом, предполагается, что ключ имеет следующий вид

$$(K_1, K_1 + 1, K_1 + 31, K_1 + 18, K_1 + 17)$$

для некоторого значения $K_1 \in \mathbb{Z}_{32}$. Теперь число вариантов для ключа равно 32, в отличие от первоначальных $32^5 = 33554432$. Перебирая возможные значения K_1, находим то, при котором получается осмысленный текст: $K_1 = 15$, ключ имеет в терминах $\mathbb{Z}_{32}$ вид $(15,16,14,1,0)$, или слово **"ПРОБА"** в терминах алфавита. Окончательный вид открытого текста следующий:

Во время этих обедов Филипп Филиппович окончательно получил звание божества. Пес

становился на задние лапы и жевал пиджак, пес изучил звонок Филиппа Филипповича - два полнозвучных отрывистых хозяйских удара, и вылетал с лаем встречать его в передней. Хозяин вваливался в чернобурой лисе, сверкая миллионом снежных блесток, пахнущий мандаринами, сигарами, духами, лимонами, бензином, одеколоном, сукном, и голос его, как командная труба, разносился по всему жилищу.[1]

В заключение заметим, что не все уравнения, получаемые указанным способом, являются верными. Например, одно из уравнений имеет вид

$$K_3 - K_4 = 10.$$

В действительности уравнение должно иметь вид

$$K_3 - K_4 = 13.$$

Оно определяется вторым по величине значением индекса, подчеркнутым в таблице волнистой чертой.

[1] М.А.Булгаков. *Собачье сердце.*

2.5. Криптоанализ шифра Хилла

Шифр Хилла труднее подвергнуть криптоанализу на основе шифртекста, но он легко поддается криптоанализу на основе выбранного открытого текста.

Предположим, что в качестве алфавита берется кольцо $\mathbb{Z}_m$. Сначала предположим, что противник знает порядок n используемой для шифрования матрицы K. Предположим, что имеется n наборов из n символов открытого текста $\mathbf{x}_j = (x_{j1}, x_{j2}, \ldots, x_{jn})$ $(1 \le j \le n)$ и известны соответствующие им наборы шифртекста $\mathbf{y}_j = e_K(\mathbf{x}_j) = (y_{j1}, y_{j2}, \ldots, x_{jn})$. Определим матрицы

$$X = \begin{pmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_{n1} & x_{n2} & \ldots & x_{nn} \end{pmatrix}, \quad Y = \begin{pmatrix} y_{11} & y_{12} & \ldots & y_{1n} \\ y_{21} & y_{22} & \ldots & y_{2n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ y_{n1} & y_{n2} & \ldots & y_{nn} \end{pmatrix}.$$

Для неизвестной матрицы K получаем матричное уравнение $Y = XK$. Если матрица X обратима, отсюда находим искомую матрицу K:

$$K = X^{-1}Y.$$

Если матрица X необратима, нужна дополнительная информация указанного выше вида.

ПРИМЕР. Рассмотрим Предположим, что открытый текст **"всегда"** с помощью шифра Хилла с $n = 2$ преобразован в шифртекст **"КСЫЬМЬ"**.

Имеем следующую информацию:

$$e_K(2,17) = (10,17),\ e_K(5,3) = (27,28),\ e_K(4,0) = (12,28).$$

Вводим в рассмотрение матрицы

$$X = \begin{pmatrix} 2 & 17 \\ 5 & 3 \end{pmatrix}, \quad Y = \begin{pmatrix} 10 & 17 \\ 27 & 28 \end{pmatrix}.$$

Легко убедиться в том, что матрица X обратима (в кольце квадратных матриц второго порядка с элементами из $\mathbb{Z}_{32}$), и

$$X^{-1} = \begin{pmatrix} 19 & 31 \\ 11 & 2 \end{pmatrix}.$$

Тогда

$$K = X^{-1}Y = \begin{pmatrix} 19 & 31 \\ 11 & 2 \end{pmatrix}\begin{pmatrix} 10 & 17 \\ 27 & 28 \end{pmatrix} = \begin{pmatrix} 3 & 7 \\ 4 & 19 \end{pmatrix}.$$

Этот результат можно проверить на третьей найденной паре открытый текст — шифртекст.

Допустим, что криптоаналитик не знает порядок n используемой матрицы. Предполагая, что это значение не слишком велико, можно последовательно исследовать значения $n = 2, 3, \ldots$. В качестве контроля можно взять пары **"открытый текст — шифртекст"**, которые не были использованы для нахождения матрицы K.

2.6. Шифр гаммирования

Как и выше, будем предполагать, что рассматриваемый алфавит отождествлен с элементами кольца $\mathbb{Z}_m$. Выберем некоторую последовательность $\boldsymbol{\gamma} = \gamma_1\gamma_2\ldots\gamma_l$ элементов из $\mathbb{Z}_m$. Предположим также, что длина этой последовательности больше или равна длине предполагаемого открытого текста. Шифрование открытого текста

$$\mathbf{x} = x_1x_2\ldots x_n \quad (k \le l)$$

проведем по правилу

$$y_i = x_i + \gamma_i, \quad i = 1,2,\ldots,n,$$

где операция сложения выполняется по модулю m.

Такой шифр называется шифром *гаммирования*, последовательность $\boldsymbol{\gamma}$ называется *гаммой*, а операция поэлементного сложения символов с символами гаммы — *наложением гаммы*.

Дешифрование в данном случае, очевидно, проводится по правилу

$$y_i = x_i - \gamma_i, \quad i = 1,2,\ldots,n,$$

где вычитание выполняется по модулю m.

Рассматриваемый шифр подходит под приведенное выше определения криптосистемы, если считать, что шифруются открытые тексты *фиксированной длины* n и гамма также имеет длину n, то есть полагать, что $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m^n$. Заметим, что шифр сдвига и шифр Виженера являются частными случаями шифра гаммирования (с постоянной или периодической гаммой).

Рассмотрим сначала вопрос о связи вероятностных характеристик открытого текста, гаммы и шифртекста. Обозначим через x, γ и y слу-

чайные величины "символ открытого текста", "символ гаммы" и "символ шифртекста". Пусть p_i (q_i, r_i), $i \in \mathbb{Z}_m$ — вероятность того, что случайная величина x (соответственно γ, y) принимает значение, равное i. Напомним, в частности, что выполняется равенство $\sum_{i=0}^{m-1} p_i = 1$. Сделаем стандартнее предположение, что случайные величины x, γ являются *независимыми.*

Вероятность того, что случайная величина y принимает значение i обозначена нами через r_i. Это происходит в том (и только том) случае, когда случайная величина γ принимает значение j при некотором значении $j \in \mathbb{Z}_m$, а случайная величина x принимает значение $i - j$, где разность берется в смысле $\mathbb{Z}_m$. При фиксированном значении j первое событие происходит с вероятностью q_j, а второе — с вероятностью p_{i-j}. Поскольку эти события независимы, вероятность их одновременного появления (произведение событий) равна $p_{i-j}q_j$. Тогда величина r_i может быть найдена по формуле

$$r_i = \sum_{j=0}^{m-1} p_{i-j}q_j, \quad i = 0,1,\ldots,m-1,$$

где разность индексов берется в $\mathbb{Z}_m$.

Из этой формулы получаем следующий важный результат.

ТЕОРЕМА. *Если в гамме используются все элементы множества $\mathbb{Z}_m$ с равными вероятностями, то при любом вероятностном распределении символов открытого текста в шифртексте присутствуют все символы множества $\mathbb{Z}_m$ с равными вероятностями.*

ДОКАЗАТЕЛЬСТВО. Условие теоремы означает, что $q_i = 1/m$ для любого $i \in \mathbb{Z}_m$. Подставляя это значение в приведенную выше формулу, для произвольного $i \in \mathbb{Z}_m$ получаем:

$$r_i = \frac{1}{m} \sum_{j=0}^{m-1} p_{i-j}.$$

При фиксированном $i \in \mathbb{Z}_m$ разности $i - j$, $j \in \mathbb{Z}_m$ пробегают все множество $\mathbb{Z}_m$. Поэтому

$$\sum_{j=0}^{m-1} p_{i-j} = \sum_{j=0}^{m-1} p_j = 1.$$

Окончательно получаем, что $r_i = 1/m$ для любого $i \in \mathbb{Z}_m$.

Теорема доказана.

В силу этой теоремы, частотные характеристики открытого текста "исчезают" в шифртексте, и к нему не могут быть применены рассмотренные выше методы частотного анализа букв шифртекста.

ЗАМЕЧАНИЕ. Последнее не означает, что даже в случае использования в гамме всех символов с равными вероятностями шифртекст не может быть успешно подвергнут криптоанализу. Например, предположим, что в рассматриваемом случае алфавита $\mathbb{Z}_m$ мы берем шифр Виженера с ключевым словом длины m, в котором присутствуют *все* элементы множества $\mathbb{Z}_m$ (разумеется, по одному разу). Тогда, рассматривая этот шифр как шифр гаммирования, получаем, что гамма является периодической длины m, и при шифровании открытого текста достаточно большой длины гамма удовлетворяет условию теоремы. Однако, как мы видели выше, шифр Виженера может быть успешно подвергнут криптоанализу.

Предположим теперь, что символы гаммы не являются равновероятной. Посмотрим, какую информацию можно извлечь из анализа шифртекста.

Допустим, что нам известны распределение частот в открытом тексте и шифртексте, то есть значения p_i и r_i, $i = 0, 1, \ldots, m-1$. Тогда выписанные выше соотношения

$$r_i = \sum_{j=0}^{m-1} p_{i-j} q_j, \quad i = 0,1,\ldots,m-1$$

могут рассматриваться как система линейных уравнений с неизвестными q_i, $i = 0, 1, \ldots, m-1$. Матрица рассматриваемой системы имеет вид

$$P = \begin{pmatrix} p_0 & p_{m-1} & p_{m-2} & \cdots & p_1 \\ p_1 & p_0 & p_{m-1} & \cdots & p_2 \\ p_2 & p_1 & p_0 & \cdots & p_3 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{m-1} & p_{m-1} & p_{m-3} & \cdots & p_0 \end{pmatrix}.$$

Такая матрица называется *циркулянтом.* В ней каждая строка получается из предыдущей строки путем циклического сдвига вправо. Если эта матрица имеет ненулевой определитель, то она обратима, и рассматриваемая система линейных уравнений имеет единственное решение.

Глава 3. Теория Шеннона

3.1. Абсолютная стойкость

При обсуждении вопроса о степени безопасности криптосистемы могут быть использованы следующие два основных подхода.

Вычислительная стойкость

Эта характеристика определяет объем вычислений, требуемых для взлома криптосистемы. Криптосистема может быть названа *вычислительно стойкой,* если наилучший алгоритм для ее взлома требует по крайней мере N операций, где N — некоторое достаточно большое число. Проблема, однако, состоит в том, что ни для одной из используемых на практике криптосистем стойкость в смысле этого определения не доказана. На практике криптосистема считается вычислительно стойкой, если самый лучший из *известных* методов ее взлома требует неприемлемо большого объема вычислений (конечно, это весьма отличается от доказательства вычислительной стойкости). Другой подход состоит в сведении вопроса о вычислительной стойкости к некоторой хорошо изученной задаче, которая *считается* трудной. Например, может быть доказано утверждение следующего типа: "данная криптосистема является стойкой, если данное натуральное число n не может быть разложено на простые множители". Криптосистемы этого типа иногда называются "доказуемо стойкими". Разумеется, это также далеко от доказательства вычислительной стойкости.

Безусловная стойкость

В этом случае никаких ограничений на объем вычислений не делается. Криптосистема называется *безусловно стойкой,* если она не может быть взломана при использовании сколь угодно больших вычислительных ресурсов.

При обсуждении вопроса о стойкости криптосистемы следует сначала выбрать тип атаки. Выше мы видели, что шифры сдвига, подстановки и шифр Виженера не являются вычислительно стойкими при криптоанализе на основе шифртекста (в предположении, что объем шифртекста достаточно велик).

Здесь мы рассмотрим криптосистемы, являющиеся безусловно стойкими при криптоанализе на основе шифртекста. В частности, будет доказано, что три указанные выше криптосистемы являются безусловно стойкими, *если данным ключом шифруется только один элемент открытого текста.*

Естественным аппаратом для изучения безусловной стойкости является теория вероятностей.

Напомним некоторые элементарные факты теории вероятностей.

Мы будем рассматривать всюду далее дискретные случайные величины, принимающие конечное множество значений. Множество значений случайной величины $\mathbf{X}$ будем также обозначать через $\mathbf{X}$. Что имеется в виду в данном случае будет ясно из контекста.

Пусть $\mathbf{X}$ и $\mathbf{Y}$ — случайные величины. Вероятность того, что величина $\mathbf{X}$ принимает значение x обозначим через $\mathbf{P}(\mathbf{X}=x)$. *Совместную вероятность* того, что величина $\mathbf{X}$ принимает значение x, а величина $\mathbf{Y}$ принимает значение y обозначим через $\mathbf{P}(\mathbf{X}=x,\mathbf{Y}=y)$. *Условная вероятность* $\mathbf{P}(\mathbf{X}=x\,|\,\mathbf{Y}=y)$ — это вероятность того, что случайная величина $\mathbf{X}$ принимает значение x *при условии того,* что случайная величина $\mathbf{Y}$ приняла значение y. Две случайные величины $\mathbf{X}$ и $\mathbf{Y}$ называются *независимыми,* если

$$\mathbf{P}(\mathbf{X}=x,\mathbf{Y}=y)=\mathbf{P}(\mathbf{X}=x)\mathbf{P}(\mathbf{Y}=y)$$

для любых их возможных значений.

Имеет место следующее соотношение

$$\mathbf{P}(\mathbf{X}=x,\mathbf{Y}=y)=\mathbf{P}(\mathbf{X}=x)\mathbf{P}(\mathbf{Y}=y\,|\,\mathbf{X}=x),$$

называемое *теоремой об умножении вероятностей*. Меняя местами $\mathbf{X}$ и $\mathbf{Y}$, получаем:

$$\mathbf{P}(\mathbf{X}=x,\mathbf{Y}=y)=\mathbf{P}(\mathbf{Y}=y)\mathbf{P}(\mathbf{X}=x\,|\,\mathbf{Y}=y\,|).$$

Приравнивая правые части, сразу получаем следующее соотношение:

$$\mathbf{P}(\mathbf{X}=x\,|\,\mathbf{Y}=y)=\frac{\mathbf{P}(\mathbf{X}=x)\mathbf{P}(\mathbf{Y}=y\,|\,\mathbf{X}=x)}{\mathbf{P}(\mathbf{Y}=y)}$$

в предположении, что $\mathbf{P}(\mathbf{Y}=y)>0$. Полученное равенство называется *формулой Бейеса*. Из теоремы об умножении вероятностей получаем такое утверждение.

Для случайных величин $\mathbf{X}$ *и* $\mathbf{Y}$ *следующие условия равносильны:*

1) эти величины независимы;

2) для любых значений этих случайных величин

$$\mathbf{P}(\mathbf{X}=x\,|\,\mathbf{Y}=y)=\mathbf{P}(\mathbf{X}=x);$$

3) для любых значений этих случайных величин

$$\mathbf{P}(\mathbf{Y}=y\,|\,\mathbf{X}=x)=\mathbf{P}(\mathbf{Y}=y).$$

Рассмотрим произвольную криптосистему $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$. Обозначим вероятность того, что символ открытого текста принимает значение, равное x, через $p_{\mathcal{P}}(x)$. Будем также предполагать, что ключ K выбирается некоторым случайным образом с известным распределением вероятностей. Обозначим вероятность выбора ключа K через $p_{\mathcal{K}}(K)$. В силу описанной выше процедуры выбора ключей, естественно предполагать, что ключ K и открытый текст x являются *независимыми* случайными величинами.

Законы распределения в $\mathcal{P}$ и $\mathcal{K}$ однозначно определяют закон распределения в $\mathcal{C}$. Найдем вероятность $p_{\mathcal{C}}(y)$ того, что был передан шифртекст y. Для $K\in\mathcal{K}$ обозначим:

$$E(K)=\{e_K(x): x\in\mathcal{P}\}.$$

Иначе говоря, $E(K)$ — это множество всех возможных шифртекстов, получаемых с помощью шифрования с ключом K. Для произвольного $y\in\mathcal{C}$ по формуле полной вероятности получаем:

$$p_{\mathcal{C}}(y)=\sum_{\{K:\, y\in E(K)\}} p_{\mathcal{K}}(K)\,p_{\mathcal{P}}(d_K(y)).$$

Для произвольных $y\in\mathcal{C}$, $x\in\mathcal{P}$ условная вероятность $p_{\mathcal{C}}(y\,|\,x)$ (то есть вероятность того, что шифртекстом будет y *при условии,* что открытым текстом является x) может быть найдена по формуле:

$$p_{\mathcal{C}}(y\,|\,x)=\sum_{\{K:\, x=d_K(y)\}} p_{\mathcal{K}}(K).$$

Теперь по формуле Бейеса находим условную вероятность $p_{\mathcal{P}}(x\,|\,y)$ (то есть вероятность того, что открытым текстом будет x *при условии,* что шифртекстом является y):

$$p_{\mathcal{P}}(x\,|\,y)=\frac{p_{\mathcal{P}}(x)\,p_{\mathcal{C}}(y\,|\,x)}{p_{\mathcal{C}}(y)},$$

$$p_{\mathcal{P}}(x\,|\,y)=\frac{p_{\mathcal{P}}(x)\sum\limits_{\{K:\, x=d_K(y)\}} p_{\mathcal{K}}(K)}{\sum\limits_{\{K:\, y\in E(K)\}} p_{\mathcal{K}}(K)\,p_{\mathcal{P}}(d_K(y))}.$$

Заметим, что для проведения всех этих вычислений достаточно знать только распределения вероятностей.

Введем теперь понятие *абсолютной стойкости* криптосистемы. Это свойство означает, что нарушитель не может получить какой-либо информации об открытом тексте, зная шифртекст. Точная формулировка дается следующим определением.

ОПРЕДЕЛЕНИЕ. *Криптосистема называется абсолютно стойкой, если* $p_{\mathcal{P}}(x \mid y) = p_{\mathcal{P}}(x)$ *для любых* $x \in \mathcal{P}$, $y \in \mathcal{C}$.

Иначе говоря, апостериорная (условная) вероятность того, что открытый текст совпадает с x при условии, что шифртекст совпадает с y, равна априорной вероятности того, что открытый текст совпадает с x.

В следующем утверждении будет доказано, что шифр сдвига является абсолютно стойким. Будем предполагать, что в качестве открытого текста и шифртекста берется множество $\mathbb{Z}_m$.

ТЕОРЕМА 1. *Предположим, что в шифре сдвига все возможные ключи являются равновероятными. Тогда для любого распределения вероятностей открытого текста шифр сдвига является абсолютно стойким.*

ДОКАЗАТЕЛЬСТВО. Напомним, что в шифре сдвига

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m, \quad e_K(x) = x + K,$$

где сложение выполняется в кольце $\mathbb{Z}_m$.

По условию теоремы $p_{\mathcal{K}}(K) = 1/m$ для любого $K \in \mathcal{K}$. Прежде всего, найдем закон распределения для множества $\mathcal{C}$. Пусть $y \in \mathbb{Z}_m$. Тогда

$$p_{\mathcal{C}}(y) = \sum_{K \in \mathbb{Z}_m} p_{\mathcal{K}}(K) p_{\mathcal{P}}(d_K(y)) = \sum_{K \in \mathbb{Z}_m} \frac{1}{m} p_{\mathcal{P}}(y - K) = \frac{1}{m},$$

поскольку при фиксированном $y \in \mathbb{Z}_m$ элементы $y - K$, $K \in \mathbb{Z}_m$ пробегают все множество $\mathbb{Z}_m$ и выполняется равенство

$$\sum_{y \in \mathbb{Z}_m} p_{\mathcal{P}}(y) = 1.$$

Для любых $x \in \mathcal{P}$, $y \in \mathcal{C}$ существует единственный ключ $K \in \mathcal{K}$, такой, что $e_K(x) = y$, именно, $K = y - x$. Отсюда получаем, что

$$p_{\mathcal{C}}(y \mid x) = p_K(y - x) = \frac{1}{m}.$$

Теперь по формуле Бейеса находим:

$$p_{\mathcal{P}}(x \mid y) = \frac{p_{\mathcal{P}}(x)\, p_{\mathcal{C}}(y \mid x)}{p_{\mathcal{C}}(y)} = p_{\mathcal{P}}(x),$$

поскольку $p_{\mathcal{C}}(y \mid x) = p_{\mathcal{C}}(y) (= 1/m)$, что и доказывает абсолютную стойкость.

Теорема доказана.

Итак, шифр сдвига нельзя "взломать", если для каждого символа открытого текста используется свой ключ, *выбираемый случайным образом.*

Рассмотрим более подробно абсолютно стойкую криптосистему.

Прежде всего, отметим, что, в силу симметричности свойства независимости случайных величин, соотношение $p_{\mathcal{P}}(x \mid y) = p_{\mathcal{P}}(x)$, выполняющееся для всех $x \in \mathcal{P}$, $y \in \mathcal{C}$, равносильно тому, что для всех $x \in \mathcal{P}$, $y \in \mathcal{C}$ выполняется равенство $p_{\mathcal{C}}(y \mid x) = p_{\mathcal{C}}(y)$. Будем также предполагать, что для любого $y \in \mathcal{C}$ $p_{\mathcal{C}}(y) > 0$. Действительно, если для некоторого элемента $y \in \mathcal{C}$ выполняется равенство $p_{\mathcal{C}}(y) = 0$, то этот элемент никогда не появляется и может быть исключен из множества $\mathcal{C}$.

Зафиксируем произвольный элемент $x \in \mathcal{P}$. Для любого $y \in \mathcal{C}$ имеем: $p_{\mathcal{C}}(y \mid x) = p_{\mathcal{C}}(y) > 0$. Следовательно, существует хотя бы один элемент $K \in \mathcal{K}$, такой, что $e_K(x) = y$. Зададим отображение $\alpha : \mathcal{C} \to \mathcal{K}$, сопоставляя элементу $y \in \mathcal{C}$ произвольный элемент $K \in \mathcal{K}$ с указанным свойством. Отображение α является инъективным. Действительно, допустим, что $\alpha(y_1) = \alpha(y_2) = K$. По определению отображения α это означает, что $e_K(x) = y_1$ и $e_K(x) = y_2$ и, следовательно, $y_1 = y_2$. Из инъективности отображения α следует неравенство $|\mathcal{C}| \leq |\mathcal{K}|$. Для любого $K \in \mathcal{K}$ отображение шифрования $e_K : \mathcal{P} \to \mathcal{C}$ является инъективным. Отсюда следует оценка $|\mathcal{P}| \leq |\mathcal{C}|$. Окончательно получаем оценки

$|\mathcal{P}| \le |\mathcal{C}| \le |\mathcal{K}|$. Приведем для случая $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$ критерий абсолютной стойкости криптосистемы, принадлежащий К. Шеннону.

ТЕОРЕМА 2. *Предположим, что для криптосистемы* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *выполняется равенство* $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. *Эта криптосистема является абсолютно стойкой в том и только том случае, когда все ключи выбираются с равными вероятностями и для любых* $x \in \mathcal{P}$, $y \in \mathcal{C}$ *существует единственный ключ* $K \in \mathcal{K}$, *такой, что* $e_K(x) = y$.

ДОКАЗАТЕЛЬСТВО. Допустим, что рассматриваемая криптосистема является абсолютно стойкой. Зафиксируем произвольный элемент $x_0 \in \mathcal{P}$. В силу сказанного выше, для любого $y \in \mathcal{C}$ найдется такой элемент $K \in \mathcal{K}$, что $e_K(x_0) = y$. Это означает, что отображение $\varphi : K \to \mathcal{C}$, действующее по правилу $\varphi(K) = e_K(x_0)$, является *сюръективным* (то есть $\varphi(\mathcal{K}) = \mathcal{C}$). Учитывая еще, что $|\mathcal{K}| = |\mathcal{C}|$, отсюда выводим, что это отображение является также *инъективным*, то есть для любого $y \in \mathcal{C}$ существует *единственный* элемент $K \in \mathcal{K}$, что $e_K(x_0) = y$.

Обозначим: $n = |\mathcal{P}| (= |\mathcal{C}| = |\mathcal{K}|)$, пусть $\mathcal{P} = \{x_1, x_2, \ldots, x_n\}$. Зафиксируем элемент $y_0 \in \mathcal{C}$. Перенумеруем элементы множества $\mathcal{K}$ так, чтобы выполнялись равенства $e_{K_i}(x_i) = y_0$, $i = 1, 2, \ldots, n$. В силу независимости случайных величин x и K, имеет место равенство $p_{\mathcal{C}}(y_0 \mid x_i) = p_{\mathcal{K}}(K_i)$. С другой стороны, $p_{\mathcal{C}}(y_0 \mid x_i) = p_{\mathcal{C}}(y_0)$. Отсюда получаем:

$$p_{\mathcal{K}}(K_i) = p_{\mathcal{C}}(y_0), \quad 1 \le i \le n,$$

то есть все ключи являются *равновероятными* (и вероятность любого из них равна $1/n$).

Обратно. Предположим, что все ключи выбираются с равными вероятностями и для любых $x \in \mathcal{P}$, $y \in \mathcal{C}$ существует единственный ключ $K \in \mathcal{K}$, такой,

что $e_K(x) = y$. Докажем, что криптосистема является абсолютно стойкой при любом распределении вероятностей на множестве $\mathcal{P}$. Доказательство этого утверждения аналогично рассмотренному выше доказательству абсолютной стойкости шифра сдвига.

Пусть $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = n$. По условию $p_{\mathcal{K}}(K) = 1/n$ для любого $K \in \mathcal{K}$. Найдем закон распределения для множества $\mathcal{C}$. Пусть $y \in \mathcal{C}$. Из условия получаем: если элемент $y \in \mathcal{C}$ является фиксированным, а ключи K пробегают все множество $\mathcal{K}$, то элементы $d_K(y)$ пробегают все множество $\mathcal{P}$, принимая каждое значение по одному разу. Тогда

$$p_{\mathcal{C}}(y) = \sum_{K \in \mathcal{K}} p_{\mathcal{K}}(K) p_{\mathcal{P}}(d_K(y)) = \frac{1}{n} \sum_{x \in \mathcal{P}} p_{\mathcal{P}}(x) = \frac{1}{n}.$$

Выбреем $x \in \mathcal{P}$ и $y \in \mathcal{C}$. Пусть $K \in \mathcal{K}$ —единственный ключ, такой, что $e_K(x) = y$. Тогда

$$p_{\mathcal{C}}(y \mid x) = p_{\mathcal{K}}(K) = \frac{1}{n}.$$

Теперь по формуле Бейеса находим:

$$p_{\mathcal{P}}(x \mid y) = \frac{p_{\mathcal{P}}(x) p_{\mathcal{C}}(y \mid x)}{p_{\mathcal{C}}(y)} = p_{\mathcal{P}}(x),$$

поскольку $p_{\mathcal{C}}(y \mid x) = p_{\mathcal{C}}(y) (= 1/n)$, что и доказывает абсолютную стойкость.

Теорема доказана.

3.2. Энтропия

Наводящие соображения

В предыдущем разделе мы обсудили понятие абсолютной стойкости. Был рассмотрен частный случаем, когда ключ использовался для шифрования только один раз. Здесь будет рассмотрен другой случай, когда для шифрования открытых текстов несколько раз используется один и тот же ключ, и проанализирован вопрос о стойкости криптосистемы в случае криптоанализа на основе известного шифртекста.

Рассмотрение этого вопроса будет основано на понятии *энтропии.* Пусть $\mathbf{X}$ — дискретная случайная величина, принимающая конечное число значений. Энтропия случайной величины является математической мерой количества информации, предоставляемой наблюдением за этой величиной. Эквивалентно, это мера неопределенности исхода наблюдения за случайной величиной. Энтропия также полезна для оценки среднего числа бит, требуемого для *кодирования* элементов $\mathbf{X}$. Точные определения энтропии и кодирования будут даны ниже.

Рассмотрим случайную величину $\mathbf{X}$ которая является числом выпадений «орла» при однократном бросании монеты. Эта величина может принимать значения 0 и 1. Если монета несимметричная и все время выпадает «орлом», то случайная величина $\mathbf{X}$ всегда принимает значение, равное единице. В этом случае предстоящее испытание неопределенности не имеет, а результат проведенного испытания не несет никакой дополнительной информации: мы о нем знали заранее. Максимальная неопределенность исхода испытания имеет место

в «идеальном» случае, когда выпадение «орла» и «решки» равновероятно, то есть величина X принимает каждое из значений 0 и 1 с вероятностью $1/2$.

Рассмотрим теперь эту же ситуацию по-другому. Предположим, что монета является «идеальной». Можно сказать, что однократное бросание этой монеты, дает объем информации, равный одному *биту*, поскольку можно обозначить, например, выпадение «орла» единицей, а «решки» — нулем. Аналогично объем информации, предоставляемый n независимыми бросаниями идеальной монеты равен n, поскольку общий результат может быть записан в виде *битовой строки* длины n.

Рассмотрим несколько более общий пример. Предположим, что случайная величина $\mathbf{X}$ может принимать три различных значения x_1, x_2 и x_3 с вероятностями соответственно $1/2$, $1/4$ и $1/4$. При кодировании принимаемых случайной величиной значений строками из нулей и единиц естественно закодировать часто встречающиеся значения более короткими строками, а редко встречающиеся — более длинными. В данном случае наиболее эффективный способ кодирования следующий: x_1 кодируем символом 0, x_2 — строкой 10, x_3 — строкой 11. Тогда математическое ожидание длины кодирующей строки равно следующей величине:

$$\frac{1}{2}\times 1+\frac{1}{4}\times 2+\frac{1}{4}\times 2=\frac{3}{2}.$$

Приведенный пример позволяет сделать следующий вывод: если вероятность появления события равна 2^{-n}, то его можно закодировать битовой строкой длины n. Обобщая этот случай, можно сказать, что для кодирования события, вероятность наступления которого равна p, требуется битовая строка длины приблизительно $-\log_2 p$. Тогда для случайной величины, принимающей n раз-

личных значений с вероятностями p_1, p_2, …, p_n, математическое ожидание длины кодирующей битовой строки будет равно

$$-\sum_i p_i \log_2 p_i.$$

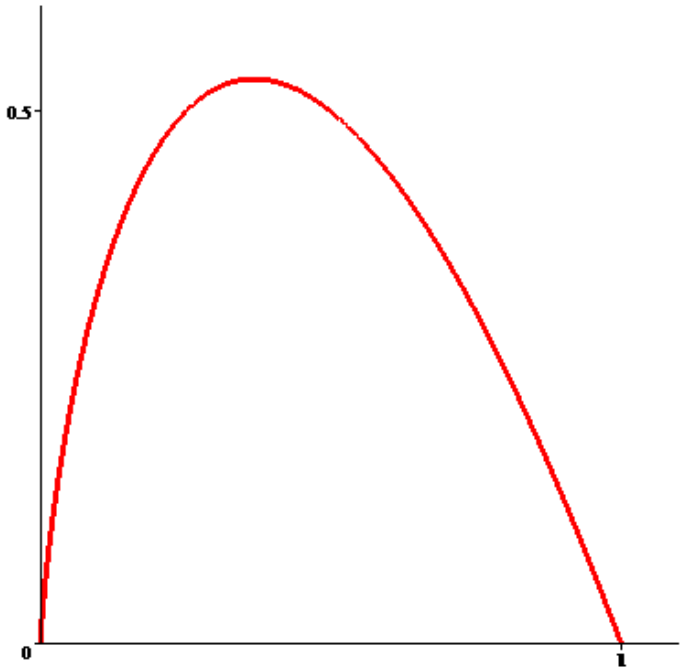
Приведенные соображения являются мотивировкой определения энтропии.

Определение энтропии

Ниже будет использоваться функция

$$f(x) = -x\log_2 x = x\log_2 \frac{1}{x}, \quad 0 < x \le 1.$$

Удобно *доопределить* эту функцию, полагая $f(0) = 0$ (в курсе математического анализа доказывается, что $\lim\limits_{x \to +0} f(x) = 0$). Тогда функция становиться непрерывной на отрезке $[0,1]$. График функции f приведен на следующем рисунке.



В дальнейшем будем писать $-p\log_2 p$, предполагая, что $0 \le p \le 1$ и имея в виду именно такое доопределение указанной функции. Подчеркнем, что ра-

венство $-p\log_2 p = 0$ равносильно тому, что $p = 0$ или $p = 1$. Для значений p, удовлетворяющих условию $0 < p < 1$ выполняется неравенство $-p\log_2 p > 0$.

Для случайной величины X в дальнейшем будем обозначать через $\mathcal{X}$ множество принимаемых ей значений. Аналогичный смысл будут иметь обозначения $\mathcal{Y}$, $\mathcal{Z}$ для случайных величин Y и Z соответственно.

ОПРЕДЕЛЕНИЕ. Энтропией случайной величины X называется величина $-\sum_{x\in\mathcal{X}} \mathbf{P}(X = x)\log_2 \mathbf{P}(X = x)$.

Запишем определение энтропии по-иному. Пусть X — случайная величина, принимающая значения x_1, x_2, …, x_n с вероятностями p_1, p_2, …, p_n соответственно. Напомним, что при этом должно выполняться равенство $\sum_{i=1}^{n} p_i = 1$. Тогда энтропия случайной величины X находится по формуле $-\sum_{i=1}^{n} p_i \log_2 p_i$.

Энтропия случайной величины X обозначается через $H(X)$. Для любого значения i выполняется неравенство $-p_i \log_2 p_i \geq 0$. Отсюда следует, что энтропия всегда принимает неотрицательные значения.

Рассмотрим некоторые свойства энтропии. Для анализа потребуются следующие вспомогательные утверждения.

ЛЕММА 1. *Для любого* $x > 0$ *имеет место неравенство* $\ln x \leq x - 1$, *причем равенство имеет место тогда и только тогда, когда* $x = 1$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим функцию $\varphi(x) = \ln x - (x - 1)$, $x > 0$. Из равенства

$$\varphi'(x) = \frac{1}{x} - 1$$

выводим, что при $0 < x < 1$ имеет место неравенство $\varphi'(x) > 0$, и, следовательно, функция φ строго возрастает на промежутке $(0,1)$. Если $x > 1$, то $\varphi'(x) < 0$, и функция φ строго убывает на промежутке $(1,+\infty)$. Поэтому для любого $x > 0$, $x \neq 1$ выполняется неравенство $\varphi(x) < \varphi(1) = 0$.

Лемма доказана.

ЛЕММА 2. *Пусть* p_1, p_2, …, p_n *и* q_1, q_2, …, q_n — *положительные числа, удовлетворяющие условиям*

$$\sum_{i=1}^{n} p_i = 1, \quad \sum_{i=1}^{n} q_i = 1.$$

Тогда имеет место оценка

$$-\sum_{i=1}^{n} p_i \log_2 p_i \le -\sum_{i=1}^{n} p_i \log_2 q_i,$$

причем равенство имеет место тогда и только тогда, когда для всех значений $i = 1, 2, \ldots, n$ *выполняется равенство* $p_i = q_i$.

ДОКАЗАТЕЛЬСТВО. Учитывая, что для любого $x > 0$ имеет место равенство $\log_2 x = \log_2 e \cdot \ln x$, доказываемое неравенство равносильно неравенству

$$-\sum_{i=1}^{n} p_i \ln p_i \le -\sum_{i=1}^{n} p_i \ln q_i,$$

которое, в свою очередь, равносильно неравенству

$$\sum_{i=1}^{n} p_i \ln \frac{q_i}{p_i} \le 0.$$

Докажем последнее соотношение. Оценивая в левой части логарифм под знаком суммы с помощью леммы 1, получаем:

$$\sum_{i=1}^{n} p_i \ln \frac{q_i}{p_i} \le \sum_{i=1}^{n} p_i \left(\frac{q_i}{p_i} - 1 \right) = \sum_{i=1}^{n} p_i - \sum_{i=1}^{n} q_i = 1 - 1 = 0,$$

причем равенство имеет место в том и только том случае, когда для каждого i $q_i / p_i = 1$, то есть $p_i = q_i$.

Лемма доказана.

ТЕОРЕМА 3. *Пусть X — случайная величина, принимающая n значений с вероятностями p_1, p_2,..., p_n, где $p_i \geq 0$, $1 \leq i \leq n$. Тогда*

$$H(X) \leq \log_2 n,$$

причем равенство достигается в том и только том случае, когда $p_i = 1/n$, $1 \leq i \leq n$, то есть все исходы равновероятны. Равенство $H(X) = 0$ имеет место в том и только том случае, когда случайная величина является постоянной.

ДОКАЗАТЕЛЬСТВО. Предположим сначала, что $p_i > 0$ для всех значений i. Полагая $q_i = \frac{1}{n}$ для тех же значений i, из леммы 2 выводим:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i \leq -\sum_{i=1}^{n} p_i \log_2 \frac{1}{n} = \log_2 n \cdot \sum_{i=1}^{n} p_i = \log_2 n.$$

При этом равенство достигается в том и только том случае, когда для всех значений i $p_i = q_i$, то есть $p_i = \frac{1}{n}$.

Предположим теперь, что среди значений p_i есть нулевые. Перенумеровывая в случае необходимости значения p_i, можно, не нарушая общности рассуждений, предполагать, что $p_1 > 0$, $p_2 > 0$, ..., $p_m > 0$, $p_{m+1} = 0$, ..., $p_n = 0$, где $1 \leq m \leq n-1$. По доказанному выше получаем:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i = -\sum_{i=1}^{m} p_i \log_2 p_i \leq \log_2 m < \log_2 n,$$

то есть $H(X) < \log_2 n$.

Перейдем к анализу равенства $H(X) = 0$.

Поскольку $-p_i \log_2 p_i \geq 0$ для любого i, равенство $-\sum_{i=1}^{n} p_i \log_2 p_i = 0$ равносильно тому, что $-p_i \log_2 p_i = 0$ для каждого i. Как было отмечено выше, это означает, что $p_i = 0$ или $p_i = 1$. Отсюда и из соотношения

$$\sum_{i=1}^{n} p_i = 1$$

следует, что существует такое значение i_0, что $p_{i_0} = 1$ и $p_i = 0$ для всех $i \neq i_0$. Это означает, что случайная величина принимает единственное значение с вероятностью, равной единице, то есть является постоянной.

Обратное утверждение очевидно.

Теорема доказана.

ОПРЕДЕЛЕНИЕ. Совместной энтропией случайных величин X и Y называется величина

$$H(X,Y) = -\sum_{x \in \mathcal{X}, y \in \mathcal{Y}} \mathbf{P}(X = x, Y = y) \log_2 \mathbf{P}(X = x, Y = y).$$

Очевидно, что для любых случайных величин X, Y имеет место равенство $H(X,Y) = H(Y,X)$.

Отметим также, что по аналогии с случаем энтропии $H(X)$ имеют место следующие свойства введенной функции.

1) Если случайная величина X может принимать m значений, а случайная величина Y — n значений, то имеет место оценка

$$H(X,Y) \leq \log_2(mn).$$

2) $H(X,Y) \geq 0$, причем $H(X,Y) = 0$ в том и только том случае, когда каждая из этих случайных величин является постоянной.

ТЕОРЕМА 4. *Если X и Y — случайные величины, то*

$$H(X,Y) \leq H(X) + H(Y),$$

причем равенство имеет место в том и только том случае, когда случайные величины X и Y независимы.

ДОКАЗАТЕЛЬСТВО. Предположим, что X принимает значения x_1, x_2, …, x_m, Y принимает значения y_1, y_2, …, y_n. Введем обозначения:

$$p_i = \mathbf{P}(X = x_i), \quad q_j = \mathbf{P}(Y = y_j), \quad r_{ij} = \mathbf{P}(X = x_i, Y = y_j),$$
$$i = 1, 2, \ldots, m, \quad j = 1, 2, \ldots, n.$$

Заметим, что

$$p_i = \sum_{j=1}^{n} r_{ij}, \quad 1 \le i \le m, \quad q_j = \sum_{i=1}^{m} r_{ij}, \quad 1 \le j \le n.$$

Независимость случайных величин X и Y означает выполнение равенства

$$\mathbf{P}(X = x_i, Y = y_i) = \mathbf{P}(X = x_i) \cdot \mathbf{P}(Y = y_j), \quad i = 1, 2, \ldots, m, \; j = 1, 2, \ldots, n.$$

В указанных выше обозначениях эти соотношения принимают вид:

$$r_{ij} = p_i q_j, \quad i = 1, 2, \ldots, m, \; j = 1, 2, \ldots, n.$$

Ограничимся предположением, что для любых i, j выполняется неравенство $r_{ij} > 0$.

Имеем:

$$H(X) + H(Y) = -\left(\sum_{i=1}^{m} p_i \log_2 p_i + \sum_{j=1}^{n} q_j \log_2 q_j \right) =$$

$$= -\left(\sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} \log_2 p_i + \sum_{j=1}^{n} \sum_{i=1}^{m} r_{ij} \log_2 q_j \right) = -\sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} \log_2 (p_i q_j).$$

С другой стороны,

$$H(X, Y) = -\sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} \log_2 r_{ij}.$$

Учитывая, что $\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij} = 1$, $\sum_{i=1}^{m}\sum_{j=1}^{n} p_i q_j = \sum_{i=1}^{m} p_i \cdot \sum_{j=1}^{n} q_j = 1$, из леммы 2 получаем:

$$H(X,Y) = -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij} \log_2 r_{ij} \le -\sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij} \log_2 (p_i q_j) = H(X) + H(Y),$$

причем равенство имеет место в том и только том случае, когда $r_{ij} = p_i q_j$ для всех значений индексов i и j, то есть в том и только том случае, когда случайные величины X и Y независимы.

Теорема доказана.

ОПРЕДЕЛЕНИЕ. Пусть X и Y — случайные величины, y — одно из значений, которые может принимать случайная величина Y. Условной энтропией X при условии $Y = y$ называется величина

$$H(X \mid Y = y) = -\sum_{x \in \mathcal{X}} \mathbf{P}(X = x \mid Y = y) \log_2 (\mathbf{P}(X = x \mid Y = y)).$$

Заметим, что введенная величина принимает неотрицательные значения. Проанализируем случай ее обращения в ноль. Допустим, что для некоторого y_0 имеет место равенство $H(X \mid Y = y_0) = 0$. Это означает, что для любого x

$$\mathbf{P}(X = x \mid Y = y_0) = 0 \text{ или } \mathbf{P}(X = x \mid Y = y_0) = 1.$$

Поскольку

$$\sum_{x \in \mathcal{X}} \mathbf{P}(X = x \mid Y = y_0) = 1,$$

отсюда получаем: если $Y = y_0$, то случайная величина X принимает одно и только одно значение, то есть значения случайной величины X в этом случае однозначно определены. Очевидно, что это утверждение допускает обращение: если при $Y = y_0$ случайная величина X принимает только одно значение, то $H(X \mid Y = y_0) = 0$.

Ниже нам понадобится следующее утверждение, аналогичное свойству «обычной» энтропии (теорема 3). Допустим, что при условии $Y = y_0$ случайная величина X может принимать только k значений. Тогда

$$H(X \mid Y = y_0) \le \log_2 k .$$

ОПРЕДЕЛЕНИЕ. Условной энтропией X при условии Y называется величина

$$H(X \mid Y) = \sum_{y \in \mathcal{Y}} \mathbf{P}(Y = y) H(X \mid Y = y).$$

Величина $H(X \mid Y)$ определяет степень неопределенности случайной величины X после наблюдения величины Y.

Перепишем приведенные формулу по-другому. Введем такие обозначения:

$$p(x) = \mathbf{P}(X = x), \quad p(y) = \mathbf{P}(Y = y),$$

$$p(x, y) = \mathbf{P}(X = x, Y = y), \quad p(x \mid y) = \mathbf{P}(X = x \mid Y = y).$$

Тогда

$$H(X \mid Y = y) = -\sum_{x \in \mathcal{X}} p(x \mid y) \log_2 p(x \mid y),$$

$$H(X \mid Y) = \sum_{y \in \mathcal{Y}} p(y) H(X \mid Y = y) =$$

$$= -\sum_{y \in \mathcal{Y}} p(y) \sum_{x \in \mathcal{X}} p(x \mid y) \log_2 p(x \mid y) =$$

$$= -\sum_{\substack{x \in \mathcal{X}, \\ y \in \mathcal{Y}}} (p(y) p(x \mid y)) \log_2 p(x \mid y).$$

В силу теоремы об умножении вероятностей, имеет место равенство

$$p(y) p(x \mid y) = p(x, y),$$

и окончательно:

$$H(X\,|\,Y) = -\sum_{\substack{x\in\mathcal{X},\\ y\in\mathcal{Y}}} p(x,y)\log_2 p(x\,|\,y).$$

Рассмотрим теперь некоторые свойства условной энтропии. Для любых значений y имеет место неравенство $H(X\,|\,Y=y)\geq 0$. Отсюда следует, что для любых случайных величин X и Y выполняется неравенство $H(X\,|\,Y)\geq 0$.

Пусть x_0 — произвольное значение, принимаемое случайной величиной X. По доказанному выше $H(X\,|\,X=x_0)=0$. Отсюда находим, что $H(X\,|\,X)=0$

.

Последнее свойство легко переносится на следующий более общий случай: если значения случайной величины Y однозначно определяют значения случайной величины X, то $H(X\,|\,Y)=0$.

ТЕОРЕМА 5. *Для случайных величин X и Y имеют место равенства*

$$H(X,Y) = H(Y) + H(X\,|\,Y) = H(X) + H(Y\,|\,X).$$

ДОКАЗАТЕЛЬСТВО. Учитывая соотношение $H(X,Y)=H(Y,X)$, достаточно доказать первое равенство.

По определению

$$H(X,Y) = -\sum_{x,y} p(x,y)\lo\ g\, p(x,y).$$

По теореме об умножении вероятностей

$$p(x,y) = p(y)\,p(x\,|\,y).$$

Заменяя аргумент логарифмической функции по этой формуле, получаем:

$$H(X,Y) = -\sum_{\substack{x\in X,\\ y\in\mathcal{Y}}} p(x,y)\log_2 p(y) - \sum_{\substack{x\in\mathcal{X},\\ y\in\mathcal{Y}}} p(x,y)\log_2 p(x\,|\,y).$$

Второе слагаемое в правой части равно $H(X\,|\,Y)$. Рассмотрим первой слагаемое. Перейдем в нем к повторным суммам:

$$-\sum_{\substack{x\in\mathcal{X},\\ y\in\mathcal{Y}}} p(x,y)\log_2 p(y) = -\sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{Y}} p(x,y)\right)\log_2 p(y).$$

Учитывая соотношение $\sum_{x\in\mathcal{X}} p(x,y) = p(y)$ получаем, что последняя сумма равна $H(Y)$.

Теорема доказана.

СЛЕДСТВИЕ. *Имеет место оценка* $H(X\,|\,Y) \le H(X)$, *причем равенство имеет место в том и только том случае, когда случайные величины* X *и* Y *независимы.*

Действительно, по доказанному $H(X\,|\,Y) = H(X,Y) - H(Y)$. Применяя предыдущую теорему, получаем:

$$H(X\,|\,Y) \le H(X) + H(Y) - H(Y) = H(X),$$

причем равенство имеет место в том и только том случае, когда

$$H(X,Y) = H(X) + H(Y),$$

то есть, когда X и Y независимы.

По аналогии с введенными выше понятиями могут быть определены и другие варианты определения энтропии для случаев трех и большего числа случайных величин. Например, если X, Y и Z — случайные величины, можно определить следующие объекты:

$$H(X,Y,Z), \quad H(X,Y\,|\,Z), \quad H(X\,|\,Y,Z).$$

Для этого случая справедливы аналоги доказанных выше утверждений. Например, имеет место равенство

$$H(X,Y,Z) = H(X,Y) + H(Z\,|\,X,Y),$$

при этом $H(Z\,|\,Y,Z) = 0$ в том и только том случае, когда значения, принимаемые случайными величинами Y и Z, однозначно определяют значение случайной величины X.

В заключение приведем один пример. Предположим, что испытание состоит в двукратном бросании игрального кубика, на котором с равными вероятностями выпадает одно из значений от одного до шести. Введем следующие случайные величины:

X — число очков, выпавших при первом бросании;

Y — число очков, выпавших при втором бросании;

$Z = X + Y$.

Случайные величины X и Y являются независимыми и имеют такое распределение:

X , Y	1	2	3	4	5	6
p	1/6	1/6	1/6	1/6	1/6	1/6

Отсюда получаем, что

$$H(X) = H(Y) = -\sum_{i=1}^{6} \frac{1}{6} \log_2 \frac{1}{6} = \log_2 6 \approx 2.5849625010.$$

Далее имеем: $\mathbf{P}(X = i, Y = j) = \frac{1}{36}$ для любых значений i, $j = 1, 2, \ldots, 6$. Следовательно,

$$H(X,Y) = -\sum_{i=1}^{36} \frac{1}{36} \log_2 \frac{1}{36} = \log_2 36 \approx 5.169925001.$$

В данном случае случайные величины являются независимыми, и имеет место равенство

$$H(X,Y) = H(X) + H(Y).$$

Случайная величина Z имеет следующее распределение

Z	2	3	4	5	6	7	8	9	10	11	12
p	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36

Отсюда находим, что $H(Z) \approx 3.274401919$.

Найдем значение $H(X,Z)$. Учтем, что

$$\mathbf{P}(X=i,Z=j)=\begin{cases}\mathbf{P}(Y=j-i)=\dfrac{1}{36}, & \text{если } 1\le j-i\le 6,\\ 0 & \text{в остальных случаях.}\end{cases}$$

Отсюда получаем:

$$H(X,Z)=-\sum_{\substack{1\le i\le 6,\\ 2\le j\le 12,\\ 1\le j-i\le 6}}\frac{1}{36}\log_2\frac{1}{36}=-\sum_{i=1}^{6}\sum_{j=i+1}^{i+6}\frac{1}{36}\log_2\frac{1}{36}=$$

$$=-36\cdot\frac{1}{36}\log_2\frac{1}{36}=\log_2 36\approx 5.169925001.$$

Перейдем к нахождению условных энтропий. В силу независимости случайных величин X и Y имеют место равенства

$$H(X\mid Y)=H(X),\quad H(Y\mid X)=H(Y).$$

Значения любых двух из случайных величин X, Y, Z однозначно определяют значение оставшейся величины. Поэтому

$$H(Z\mid X,Y)=0,\quad H(X\mid Z,Y)=0,\quad H(Y\mid Z,X)=0$$

Из формулы

$$H(X,Z)=H(X)+H(Z\mid X)$$

находим, что

$$H(Z\mid X)=H(X,Z)-H(X)=\log_2 36-\log_2 6=\log_2 6\approx 2.5849625010.$$

Аналогично получаем:

$$H(X\mid Z)=H(X,Z)-H(Z)\approx 1.895523082.$$


Хаффмен

3.3. Кодирование Хаффмена и энтропия

В этом разделе будет обсуждена связь между определением энтропии и так называемым кодированием Хаффмена.

Предположим, как и выше, что $\mathbf{X}$ является случайной величиной, принимающей конечное множество значений с известными вероятностями. Как и выше, через $\mathcal{X}$ будем обозначать множество всех значений, принимаемых данной случайной величиной, вероятность появления значения x обозначаем через $p(x)$.

Обозначим через $\mathrm{Str}\{0,1\}$ множество всех конечных строк, составленных из элементов 0 и 1.

ОПРЕДЕЛЕНИЕ. Кодированием случайной величины $\mathbf{X}$ называется отображение $f:\mathcal{X}\to\mathrm{Str}\{0,1\}$.

Для каждого $x\in\mathcal{X}$ битовая строка $f(x)$ называется *кодом* символа x или *кодовой строкой.*

Кодирование можно распространить на строки, составленные из элементов множества $\mathcal{X}$, полагая

$$f:x_1x_2\ldots x_n\to f(x_1)\,\&\,f(x_2)\,\&\cdots\&\,f(x_n),$$

где знак $\&$ означает конкатенацию строк.

Схема кодирования последовательностей элементов множества $\mathcal{X}$ должна обладать следующим основным свойством: она должна допускать однозначное *декодирование*, то есть восстановление исходной строки по битовой строке. Это означает, что отображение f, распространенное на строки, составленные из элементов множества $\mathcal{X}$, должно быть *инъективным*.

ПРИМЕР. Предположим, что случайная величина $\mathbf{X}$ может принимать четыре значения, a, b, c и d, то есть $\mathcal{X}=\{a,b,c,d\}$. Рассмотрим следующие три варианта кодирования:

$$f(a)=1, \quad f(b)=10, \quad f(c)=100, \quad f(d)=1000;$$
$$g(a)=0, \quad g(b)=10, \quad g(c)=110, \quad g(d)=111;$$
$$h(a)=0, \quad h(b)=01, \quad h(c)=10, \quad h(d)=11.$$

Легко убедиться в том, что отображения f и g являются инъективными кодированиями, а отображение h — нет.

Рассмотрим отображение f. Любая строка, определяемая эти отображением, может быть декодирована, например, следующим образом: начинаем от первой единицы и до нового появления единицы или конца строки, сигнализирующих о том, что все *предыдущие* символы образуют код некоторого символа.

В случае отображения g декодирование проводим последовательно, двигаясь слева направо. На каждом шаге для получаемой подстроки можно сразу сказать, кодирует она некоторый символ или нет. Например, если дана строка **`10101100111`**, переводим **`10`** в b, следующий фрагмент **`10`** снова в b, **`110`** в c, **`0`** в a, **`111`** в d. Окончательно получаем строку $bbcad$.

Отображение h не является инъективным. Достаточно указать пример: $h(ac)=h(ba)=010$.

Наиболее удобным для декодирования является отображение g. В этом случае для каждой получаемой подстроки мы сразу знаем, кодирует она некоторый символ или нет (в отличие от отображения f).

ОПРЕДЕЛЕНИЕ. Кодирование $f:\mathcal{X}\to \mathrm{Str}\{0,1\}$ называется префиксным, если не существует таких элементов x_1, $x_2\in\mathcal{X}$ и строки $s\in\mathrm{Str}\{0,1\}$ ненулевой длины, для которых выполняется равенство $f(x_1)=f(x_2)\,\&\,s$.

Приведенное определение означает, что для каждой считанной подстроки мы можем определить, является она кодовой или нет, не дожидаясь считывания следующего символа. Любое префиксное кодирование допускает однозначное декодирование. Подчеркнем, что однозначное декодирование возможно и для

кодов, не являющихся префиксными. Действительно, рассмотренное выше кодирование с помощью отображения f допускает однозначное декодирование, однако префиксным не является.

В качестве меры эффективности произвольного кодирования f значений случайной величины естественно взять математическое ожидание длины кодового слова, то есть величину

$$\ell(f) \stackrel{\text{def}}{=} \sum_{x \in \mathcal{X}} p(x) \cdot \mathrm{Len}(f(x)),$$

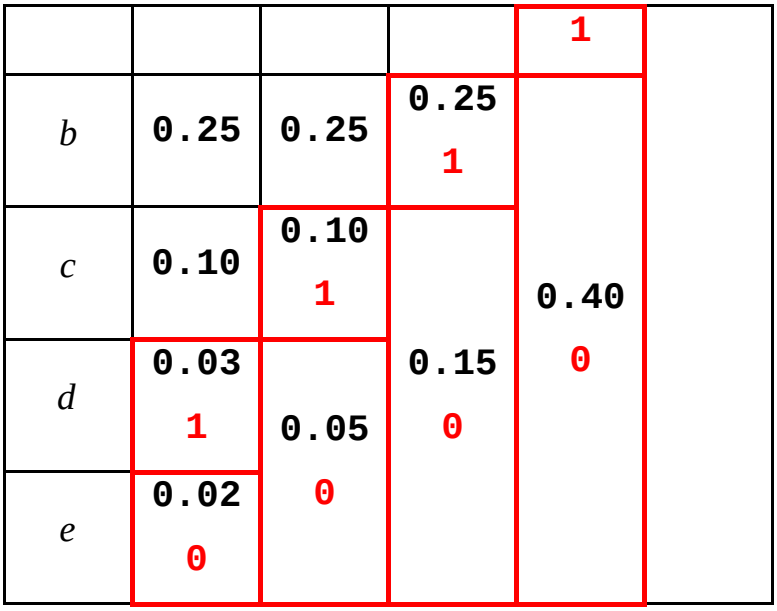
где $\mathrm{Len}(f(x))$ обозначает длину строки $f(x)$.

Задача нахождения инъективного кодирования f, минимизирующего величину $\ell(f)$ решается с помощью описываемого ниже *алгоритма Хаффмена*. Дадим неформальное описание этого алгоритма. Построение начинается с распределения вероятностей на множестве $\mathcal{X}$. На каждом шаге выбираются два элемента этого множества, имеющие наименьшие вероятности. Элементу из этих двух, имеющему меньшую вероятность сопоставляется значение **0**, второму элементу — значение **1**. Выбранные элементы объединяются в один элемент, вероятность которого полагается равной сумме вероятностей объединяемых элементов. Процесс продолжается, пока не останется *один* элемент, которому никаких значений не сопоставляется. Кодирование элементов множества $\mathcal{X}$ строится путем перехода от последнего элемента к кодируемому. Известно, что кодирование Хаффмена является префиксным и имеет место оценка

$$H(\mathbf{X}) \le \ell(f) < H(\mathbf{X}) + 1$$

Пример. Пусть $\mathcal{X} = \{a, b, c, d, e\}$, и вероятности равны соответственно 0.60, 0.25, 0.10, 0.03, 0.02. Работу алгоритма Хаффмена представим в виде следующей таблицы:

a	**0.60**	**0.60**	**0.60**	**0.60**	**1.00**



Здесь объединяемые ячейки выделены красным цветом и в них указаны сопоставляемые двоичные значения. В соответствии с указанным выше алгоритмом получаем следующее кодирование:

$$\begin{aligned} a &\to \mathtt{1} \\ b &\to \mathtt{01} \\ c &\to \mathtt{001} \\ d &\to \mathtt{0001} \\ e &\to \mathtt{0000} \end{aligned}$$

Математическое ожидание длины кодового слова равно

$$\ell(f) = 0.60\times 1 + 0.25\times 2 + 0.10\times 3 + 0.03\times 4 + 0.02\times 4 = 1.60.$$

Энтропия рассматриваемой случайной величины $H(\mathbf{X}) \approx 1.5390161$.

3.4. Ложные ключи и расстояние единственности

В этом разделе понятие энтропии будет использовано для анализа криптосистем.

Пусть $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ — произвольная криптосистема. Будем рассматривать значения символов открытого текста, шифртекста и ключа как случайные величины, которые будем обозначать соответственно через $\mathbf{P}$, $\mathbf{C}$ и $\mathbf{K}$. Множествами значений, принимаемых этими случайными величинами, являются соответственно множества $\mathcal{P}$, $\mathcal{C}$ и $\mathcal{K}$, значения, принимаемые этими случайными величинами, будут обозначаться через x, y и K. Случайные величины $\mathbf{P}$ и $\mathbf{K}$ предполагаются независимыми.

Определение. Для криптосистемы $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ условная энтропия $H(\mathbf{K}\,|\,\mathbf{C})$ называется ненадежностью ключа.

Ненадежность ключа является мерой объема информации о ключе, доставляемой шифртекстом.

Теорема. *Для произвольной криптосистемы* $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ *выполняется равенство* $H(\mathbf{K}\,|\,\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{P})$.

Доказательство. Заметим, прежде всего, что

$$H(\mathbf{K},\mathbf{P},\mathbf{C}) = H(\mathbf{C}\,|\,\mathbf{K},\mathbf{P}) + H(\mathbf{K},\mathbf{P}).$$

Рассмотрим слагаемые в правой части формулы. Открытый текст и ключ определяют шифртекст однозначно, поскольку имеет место равенство $y = e_K(x)$. Поэтому $H(\mathbf{C}\,|\,\mathbf{K},\mathbf{P}) = 0$. Учитывая независимость случайных величин $\mathbf{P}$ и $\mathbf{K}$, получаем, что $H(\mathbf{K},\mathbf{P}) = H(\mathbf{K}) + H(\mathbf{P})$. Тогда

$$H(\mathbf{K},\mathbf{P},\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}).$$

С другой стороны, имеет место равенство

$$H(\mathbf{K},\mathbf{P},\mathbf{C}) = H(\mathbf{P}\,|\,\mathbf{K},\mathbf{C}) + H(\mathbf{K},\mathbf{C}).$$

В силу равенства $x = d_K(y)$, ключ и шифртекст однозначно определяют открытый текст. Следовательно $H(\mathbf{P} \mid \mathbf{K}, \mathbf{C}) = 0$. Учтем также, что

$$H(\mathbf{K}, \mathbf{C}) = H(\mathbf{C}) + H(\mathbf{K} \mid \mathbf{C}).$$

Тогда получаем, что

$$H(\mathbf{K}, \mathbf{P}, \mathbf{C}) = H(\mathbf{C}) + H(\mathbf{K} \mid \mathbf{C}).$$

Приравнивая полученные выражения для величины $H(\mathbf{K}, \mathbf{P}, \mathbf{C})$ и выражая значение $H(\mathbf{K} \mid \mathbf{C})$, получаем искомую формулу.

Теорема доказана.

Пусть $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ — используемая криптосистема, и строка открытого текста $x_1 x_2 \ldots x_n$ с помощью *одного ключа* преобразуется в строку шифртекста $y_1 y_2 \ldots y_n$. Мы рассматриваем только криптоанализ на основе шифртекста и предполагаем, что криптоаналитик имеет бесконечные вычислительные ресурсы. Предполагается также, что открытый текст является сообщением на некотором "естественном" языке (например, русском или английском), о чем также известно криптоаналитику. Задача криптоаналитика состоит в том, чтобы выделить из некоторого набора ключей единственный верный ключ. Остальные возможные ключи называются *ложными*.

Например, допустим, что имеется шифртекст **"WNAJW"**, полученный в результате шифрования с помощью шифра сдвига. Легко убедиться в том, что ему соответствуют два «осмысленных» открытых текста — «**river**» и «**arena**», а соответствующими ключами, один из которых верный, а другой ложный, будут 5 и 22. В случае русского языка (32 буквы) шифртексту **"ПОМК"** соответствуют два открытых текста — «**едва**» и «**утро**» с ключами 10 и 28 соответственно.

Наша задача состоит в оценке математического ожидания числа ложных ключей. Сначала определим некоторую характеристику естественного языка,

определяющую средний объем информации на букву с строке осмысленного открытого текста.

В качестве первого приближения возьмем энтропию случайной величины $\mathbf{P}$ — отдельной буквы языка. Разумеется, последовательные буквы языка не являются независимыми. В английском языке после буквы **"Q"** всегда следует **"U"**, а в современном русском языке после **"Ъ"** всегда следует гласная. В качестве второго приближения возьмем энтропию вероятностного распределения всех биграмм, а затем разделим эту величину на 2. В общем случае обозначим через $\mathbf{P}^n$ случайную величину — n-грамму открытого текста. В качестве очередного приближения возьмем значение $\frac{1}{n}H(\mathbf{P}^n)$. Если алфавит открытого текста содержит m символов, то n-граммы могут теоретически принимать m^n значений, и, используя стандартные оценки для энтропии, получаем:

$$0 \le H(\mathbf{P}^n) \le \log_2 m^n = n \log_2 m.$$

Отсюда следует оценка

$$0 \le \frac{1}{n} H(\mathbf{P}^n) \le \log_2 m.$$

ОПРЕДЕЛЕНИЕ. Энтропией естественного языка L называется величина

$$H_L = \lim_{n \to +\infty} \frac{H(\mathbf{P}^n)}{n}.$$

ЗАМЕЧАНИЕ. Существование указанного предела в строгом математическом смысле можно доказать при достаточно жестких предположениях относительно случайной величины $\mathbf{P}$, не имеющих места для естественного языка. В данном случае имеется в виду значение, около которого группируются величины $\frac{H(\mathbf{P}^n)}{n}$ при больших значениях n. Именно так находится приводимое ниже значение.

Избыточностью языка L называется величина

$$R_L = 1 - \frac{H_L}{\log_2 |\mathcal{P}|}.$$

ЗАМЕЧАНИЕ. Величина H_L дает энтропию языка L, приходящуюся на один символ. Энтропией *случайного* «языка» (то есть языка, в котором все символы равновероятны и значение каждого символа не зависит от предыдущих) является величина $\log_2 |\mathcal{P}|$. Поэтому величина R_L характеризует долю "лишних символов", являющихся избыточными.

В случае английского языка полагают $R_L \approx 0.75$. Это означает, что примерно 75% букв являются избыточными. Из этого, разумеется, нельзя сделать вывод, что можно произвольным образом вычеркнуть в тексте три буквы из каждых четырех и рассчитывать, что после этого текст удастся однозначно восстановить. Такой результат можно интерпретировать так. При кодировании Хаффмена для n-грамм при достаточно большом значении n объем текста будет сжиматься примерно в четыре раза по сравнению с исходным.

Если даны распределения вероятностей на множествах $\mathcal{K}$ и $\mathcal{P}^n$, то распределение вероятностей на множестве $\mathcal{C}^n$ n-грамм шифртекста будет однозначно определено. Кроме случайной величины $\mathbf{P}^n$ — n-граммы открытого текста, будем рассматривать случайную величину $\mathbf{C}^n$ — n-грамму шифртекста. Через $p_{\mathcal{P}^n}(x)$ будем обозначать вероятность появления n-граммы открытого текста x, через $p_{\mathcal{C}^n}(y)$ будем обозначать вероятность появления n-граммы шифртекста y

Для $y \in \mathcal{C}^n$ определим следующее множество

$$K(y) = \{K \in \mathcal{K} : \exists x \in \mathcal{P}^n, \quad p_{\mathcal{P}^n}(x) > 0, \quad e_K(x) = y\}.$$

Иначе говоря, $K(y)$ есть множество всех ключей K, для которых y является результатом шифрования осмысленной строки открытого текста длины n, то есть множество всех ключей, дающих в качестве шифртекста строку y. Если y — имеющаяся строка шифртекста, то число ложных ключей равно $|K(y)|-1$, поскольку из всех ключей один и только один является верным. Математическое ожидание числа всех ложных ключей (по всем возможным строкам шифртекста) обозначим через $\bar{\varphi}_n$. Тогда

$$\bar{\varphi}_n = \sum_{y\in\mathcal{C}^n} p_{\mathcal{C}^n}(y)(|K(y)|-1) =$$

$$= \sum_{y\in\mathcal{C}^n} p_{\mathcal{C}^n}(y)|K(y)| - \underbrace{\sum_{y\in\mathcal{C}^n} p_{\mathcal{C}^n}(y)}_{=1} = \sum_{y\in\mathcal{C}^n} p_{\mathcal{C}^n}(y)|K(y)|-1.$$

В силу доказанной выше теоремы,

$$H(\mathbf{K}\,|\,\mathbf{C}^n) = H(\mathbf{K}) + H(\mathbf{P}^n) - H(\mathbf{C}^n). \qquad (*)$$

Кроме того,

$$H(\mathbf{P}^n) \approx nH_L = n(1-R_L)\log_2|\mathcal{P}|$$

при достаточно большом n. Учтем, что значения случайной величины $\mathbf{C}^n$ принадлежат множеству $\mathcal{C}^n$ и $|\mathcal{C}^n| = |\mathcal{C}|^n$. Отсюда получаем:

$$H(\mathbf{C}^n) \le \log_2|\mathcal{C}^n| = n\log_2|\mathcal{C}|.$$

Предполагая дополнительно, что $|\mathcal{P}| = |\mathcal{C}|$ из (*) выводим:

$$H(\mathbf{K}\,|\,\mathbf{C}^n) \ge H(\mathbf{K}) - nR_L\log_2|\mathcal{P}|.$$

Теперь оценим величину $H(\mathbf{K}\,|\,\mathbf{C}^n)$, пользуясь определением условной энтропии:

$$H(\mathbf{K}\,|\,\mathbf{C}^n) = \sum_{y\in\mathcal{C}^n} p_{\mathcal{C}^n}(y)H(\mathbf{K}\,|\,\mathbf{C}^n = y) \le$$

$$\le \sum_{y\in\mathcal{C}^n} p_{\mathcal{C}^n}(y)\log_2|K(y)| \le \log_2\left(\sum_{y\in\mathcal{C}^n} p_{\mathcal{C}^n}(y)|K(y)|\right) = \log_2(\overline{\varphi}_n+1).$$

Здесь учтено (знак выделен красным цветом), что при условии $\mathbf{C}^n = y$ случайная величина $\mathbf{K}$ может принимать не более $|K(y)|$ значений и, следовательно, $H(\mathbf{K}\,|\,\mathbf{C}^n = y) \le \log_2|K(y)|$.

Комбинируя полученные оценки, находим, что

$$\log_2(\overline{\varphi}_n+1) \ge H(K) - nR_L\log_2|\mathcal{P}|.$$

Предполагая дополнительно, что ключи выбираются с равными вероятностями, получаем следующий результат.

ТЕОРЕМА. *Предположим, что для криптосистемы* $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ *выполняется равенство* $|\mathcal{P}|=|\mathcal{C}|$ *и все ключи выбираются с равными вероятностями. Пусть* R_L *— избыточность языка* L. *Тогда для данной строки шифртекста достаточно большой длины* n *математическое ожидание* $\overline{\varphi}_n$ *числа ложных ключей удовлетворяет оценке*

$$\overline{s}_n \ge \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1.$$

ЗАМЕЧАНИЕ. Приведенная оценка может оказаться неточной при небольших значениях n поскольку величина $H(P^n)/n$ может плохо аппроксимировать H_L при этих значениях n.

ОПРЕДЕЛЕНИЕ. Расстоянием единственности для данной криптосистемы называется величина n_0, при которой математическое ожидание числа ложных ключей становится равным нулю, то есть это средний объем шифртекста, требуемый для однозначного нахождения ключа в предположении о неограниченных вычислительных ресурсах.

Полагая $\overline{\varphi}_n = 0$, из предыдущей теоремы находим значение расстояний единственности

$$n_0 \approx \frac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}.$$

Например, в случае шифра подстановки $|\mathcal{P}| = |\mathcal{C}| = 26$, $|\mathcal{K}| = 26!$. Беря $R_L = 0.75$, находим $n_0 \approx 25$.

Исторические сведения

Фридрих Вильгельм Казиски (1805 –1881)

Майор прусской армии, криптограф и археолог. В 1863 опубликовал книгу «Тайнопись и искусство дешифрования».

Казиски «умер даже не догадываясь о том, что произвел настоящую революцию в криптоанализе» (Дэвид Кан. Взломщики кодов. М.: «Центр-полиграф», 2000).

Обратно

Огюст Керкгоффс (1835 – 1903)

Голландский лингвист и криптограф. Автор книги "Военная криптография" (1883 г.).

Он «обладал уникальной способностью выделять главное в любом предмете и всего на 64 страницах своей книги сумел найти ответы на многие вопросы, которые встали перед криптографией в результате возникновения новых условий. При этом предложенные им решения были разумными и хорошо обоснованными.» (Дэвид Кан. Взломщики кодов. М.: «Центрполиграф», 2000).

Обратно

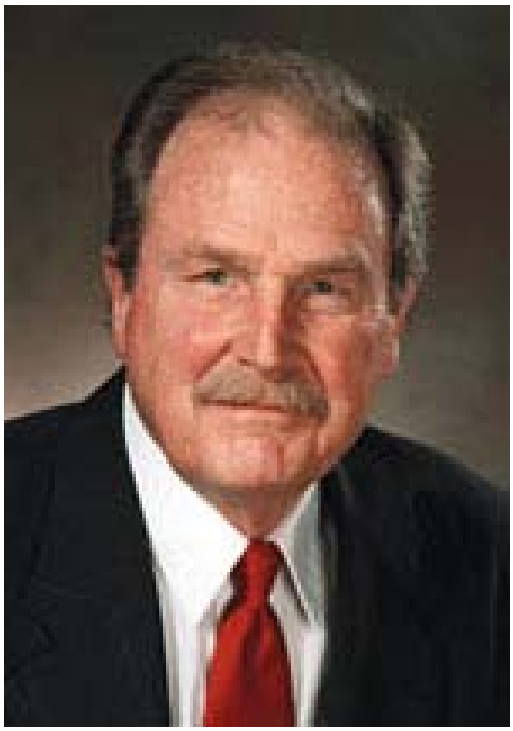
Вольф Фридман (1891 – 1969)

Вольф Фридман (Уильям Фредерик Фридман), американский криптолог и криптоаналитик, обыкновенно именуемый «отцом американской криптологии». Ввел термины «криптология» и «криптоанализ». Автор трёх учебников по военной криптографии, считающихся основополагающими текстами по этой дисциплине, и ряда научных работ по анализу кодов и шифров; пионер применения статистических методов в криптоанализе.

«Когда Фридман отнес криптоанализ к категории статистических исследований, он широко распахнул дверь в арсенал средств, которыми криптоанализ никогда прежде не располагал. Они идеально подходили для изучения статистического поведения букв и слов. … Вот почему, оглядываясь на пройденный жизненный путь, Фридман сказал, что “Индекс совпадения” является его самым важным творением. Даже одна эта работа принесла бы ему славу.» (Дэвид Кан. Взломщики кодов. М.: «Центрполиграф», 2000).

Обратно

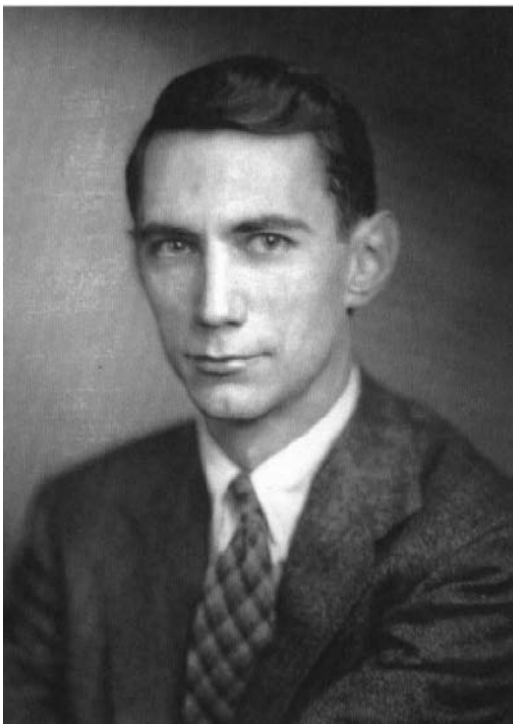
Дэвид Хаффмен (1925 – 1999)



Американский математик и инженер. Внес важный вклад теорию информации, теорию кодирования, в многие области электроники.

Обратно

Клод Элвуд Шеннон (1916 – 2001)



Американский математик и инженер, один из создателей математической теории информации. Основные работы Шеннона посвящены алгебре логики, теории релейно-контактных схем, математической теории связи, теории информации и кибернетике.

«Сила ума Шеннона, его огромный вклад в теорию шифровального дела выразились в открытии избыточности как основы криптоанализа: “Вскрытие большинства шифров становится возможным только благодаря существованию избыточности в открытых текстах”. Шеннон первым сумел объяснить постоянство частот встречаемости букв, а тем самым и такое зависящее от него явление, как криптоанализ, дав возможность глубоко понять процесс аналитического вскрытия шифров.» (Дэвид Кан. Взломщики кодов. М.: «Центрполиграф», 2000).

Рекомендуемая литература

1. Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В. Основы компьютерной стеганографии. М.: Радио и связь. 2003.
2. Аграновский А.В., Хади Р.А. Практическая криптография. Алгоритмы и их программирование. М.: СОЛОН-Пресс. 2002.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. М.: «Гелиос АРВ». 2001.
4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. М.: «Горячая линия — Телеком». 2001.
5. Брассар Ж. Современная криптология. М.: «ПОЛИМЕД». 1999.
6. Варфоломеев А.А., Жуков А.Е., Пудовкина М.А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. М.: «ПАИМС». 2000.
7. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО. 2003.
8. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: «Солон-Пресс». 2002.
9. Зубов А.Ю. Совершенные шифры. М.: «Гелиос АРВ». 2003.
10. Кан Д. Взломщики кодов. М.: «Центрполиграф», 2000.
11. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб: «Лань». 2000.
12. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). М.: Высшая школа. 1999.
13. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. М.: ДМК. 2000.
14. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: «Радио и связь». 1999.

15. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. Учебное пособие для вузов. М.: «Горячая линия-Телеком». 2005.
16. Саломаа А. Криптография с открытым ключом. М.: «Мир». 1995.
17. Ященко В.В. (ред.) Введение в криптографию. М.: «МЦНМО-ЧеРо». 1998.
18. Buchmann J. Einführung in die Kryptographie. Springer. 2008.
19. Churchhouse R.F. Codes and ciphers. Julius Caesar, the Enigma and the Internet. Cambridge University Press. 2004.
20. Goldreich O. Foundations of cryptography. Vol.1. Basic tools. Cambridge University Press. 2004.
21. Hoffstein J., Pipher J., Silverman J. H. An Introduction to Mathematical Cryptography. Springer. 2008.
22. Stinson D.R. Cryptography. Theory and practice. 3 ed. Chapman & Hall/CRC. 2006.