Лекция 5

ПРОСТЕЙШИЕ КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

История шифрования насчитывает не одно тысячелетие. Шифрованные сообщения найдены на стенах пещер первобытных людей и на стенах гробниц фараонов в Египте. Видимо, первые системы шифрования появились одновременно с письменностью в четвертом тысячелетии до нашей эры. Шифрование на протяжении долгой истории служило не только методом утаивания информации от нежелательных лиц, но способом подчеркивания ее необычности или важности.

1. Исторические примеры

1.1. Шифр атбаш. Шифрование использовалось в Библии. Некоторые фрагменты библейских текстов зашифрованы шифром *атбаш*. Правило шифрования состояло в замене i-ой буквы алфавита на букву $n - i + 1$, где n — количество букв алфавита.

1.2. Пророк Даниил. Один из самых известных примеров шифрованного текста изображен на одной из картин Рембрандта (см. рис. 1 ниже).

Этот случай описан в Ветхом Завете в книге пророка Даниила. Согласно преданию, во время пира вавилонского царя Валтасара, состоявшегося незадолго до падения Вавилона от рук Дария Мидийского, таинственная рука начертала на стене арамейские слова: "*Мене, мене, текел, упарсин*".

Объяснение этого знамения вызвало затруднения у вавилонских мудрецов, однако их смог пояснить пророк Даниил:

> Вот и значение слов: “мене” — исчислил Бог царство твое и положил конец ему; “текел” — ты взвешен на весах и найден очень легким; “упарсин” — разделено царство твое и дано Мидянам и Персам.
>
> (Дан.5:26-28)

“Пир царя Валтасара”
Рембрандт ван Рейн (1633)

В ту же ночь Валтасар был убит и Вавилон перешел под власть Дария Мидийского. Вероятно, библейский рассказ основывается на реальных событиях, сопровождавших вступление персидской армии в Вавилон в ночь на 12 октября 539 до н. э. (по крайней мере, отголоски истории пира Валтасара можно обнаружить в других ближневосточных и античных источниках).

Хотя интерпретация текста пророком Даниилом и не является дешифровкой сообщения в строгом понимании, сам он по праву может считаться первым дешифровщиком.

1.3. Мария Стюарт. Шифрование и дешифрование сыграли решающую (часто трагическую) роль в судьбе многих известных исторических персонажей. Королева Шотландии Мария I (Стюарт) некоторое время противостояла королеве Англии Елизавете I и претендовала на ее трон. Имя Марии Стюарт, законной правнучки короля Генриха VII

Английского, активно использовалось заговорщиками против Елизаветы I. В 1572 г. был раскрыт заговор Ридольфи, участники которого пытались сместить Елизавету и посадить на трон Англии Марию Стюарт. После раскрытия заговора Мария была заключена в лондонскую тюрьму Тауэр и ждала решения Елизаветы. В силу высокого положения арестантки казнь не могла состояться без наличия веских доказательств ее вины. Уже пребывая в заключении, Мария Стюарт оказалась вовлечённой в неосторожную переписку с Энтони Бабингтоном, агентом католических сил, в которой она поддержала идею заговора с целью убийства Елизаветы. Тексты писем были зашифрованы, но королеве удалось раскрыть код. Мария Стюарт предстала перед судом и была приговорена к казни. 8 февраля 1587 г. Мария Стюарт была обезглавлена в замке Фотерингей.

2. Механические шифровальные машины

С течением времени шифры усложнялись, а шифрование требовало все больше усилий. Разнообразные приспособления помогали шифровать и расшифровывать важные тексты. Мы рассмотрим несколько хорошо известных шифровальных приспособлений.

2.1. Скитала. Из Англии средних веков перенесемся в древнюю Спарту. Еще в VII веке до н. э. во время военных кампаний античные греки и спартанцы применяли *шифр Древней Спарты*. Для этого использовался прибор, называемый *скитала* и представляющий собой жезл цилиндрической формы. Узкая полоска пергамента обматывалась вокруг скиталы по спирали, а сообщение писалось строками по длине скитала. После того как длина скиталы оказывалась исчерпанной, она поворачивалась и текст писался под первой строкой. В качестве скиталы могли использоваться рукоятки мечей или копий.

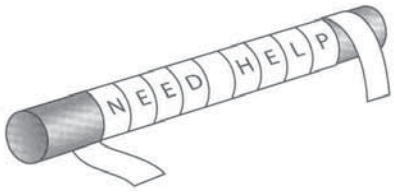


Рис. 2. Древнегреческая скитала

Например, используя скиталу, длина которой позволяет записать 5 символов, исходный текст

(1) “это шифр древней спарты”

превратится в шифрограмму

(2) “эфвптрнаоердйтшрыиес”.

Схематически шифрование текста (1) с помощью скитал можно изобразить так:

(3)

номер строки					
1:	Э	Т	О	Ш	И
2:	Ф	Р	Д	Р	Е
3:	В	Н	Е	Й	С
4:	П	А	Р	Т	Ы

На размотанной ленте сначала будут записаны буквы первого столбца в (3), затем — второго и т.д.; весь зашифрованный текст представлен в (2).

Дешифровка сообщения выполнялась с использованием скитала такого же диаметра. Однако такой шифр может быть легко взломан даже и без копии скиталы. Фактически

единственным зашифрованным параметром является диаметр скиталы. Один из методов взлома был предложен ещё Аристотелем. Он предложил использовать конус, имеющий переменный диаметр. Перемещая полоску пергамента с сообщением по длине конуса до тех пор, пока текст не начнёт читаться, мы дешифруем диаметр скиталы.

2.2. Табличка Энея. Другим шифровальным приспособлением времен Спарты была *табличка Энея*, на которой горизонтально записывались буквы алфавита в определенном порядке. При шифровании нить закреплялась у одной из сторон таблички и наматывалась вокруг нее. На каждом витке нити делалась метка напротив нужной буквы. После шифрования нить сматывалась и передавалась адресату. Ключом к этому шифру служат геометрические размеры таблички и порядок записи на ней букв алфавита. Это был довольно надежный шифр: история не сохранила документов, подтверждающих сведения о методах его вскрытия.

2.3. Шифровальное колесо Джефферсона. Описание *шифровального колеса Томаса Джефферсона*, впоследствии ставшим третьим президентом США, найдено в его бумагах, относящихся к 1795 году. Столетие спустя этот способ переоткрыл Этьен Базерис.

Рис. 3. Шифровальное колесо Джефферсона

Один из сохранившихся образцов колеса Джефферсона, который использовался армией США в 1923–1942 годах, изображен на рис. 3. Устройство состоит из 36 дисков, насаженных на общий штырь. По периметру каждого диска записаны 26 букв латинского алфавита (для каждого диска используется свой порядок букв).

Чтобы закодировать сообщение длиной не более 36 букв, каждый из дисков вращают так, чтобы на одной из строк (неважно на какой) появилось это сообщение. Теперь диски необходимо закрепить неподвижно. Сообщение шифруется соответствующими буквами любой другой строки.

Упрощенный вариант колеса с 12 дисками показан ниже. На одной из строк колеса появилось кодируемое сообщение “ATTACK AT DAWN”.

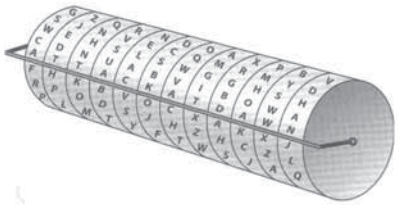


Рис. 4. Упрощенное колесо Джефферсона

Например, выберем для шифрования соседнюю строку

выше: сообщение превращается в “CDNUABVIBOWA”.

Чтобы расшифровать сообщение, адресат на одной из строк своего колеса выставляет полученный им текст “CDNUABVIBOWA”. Зафиксировав теперь положение дисков, он читает другие строки, находя осмысленное выражение “ATTACK AT DAWN” на одной из них.

Кажущаяся неоднозначность расшифрования устраняется достаточно большим числом используемых дисков. Это замечание относится лишь к осмысленным текстам. При шифровании и дешифровке неосмысленных текстов требовалась дополнительная информация.

3. Перестановочные шифры

Один из простых способов кодирования информации основан на так называемых *перестановочных шифрах*.

Идея греческой скиталы была с течением времени трансформирована в более сложные системы шифрования, в которых *ключ* к тексту сообщения определяется не диаметром скиталы, а специальной последовательностью символов. Идею можно пояснить на примере ключа “рубль” и того же текста (3):

р	**у**	**б**	**л**	**ь**
3	**4**	**1**	**2**	**5**
—	—	—	—	—
Э	Т	О	Ш	И
Ф	Р	Д	Р	Е
В	Н	Е	Й	С
П	А	Р	Т	Ы

Символы ключа определяют определенный порядок, в котором столбцы текста записываются в шифрованном виде. В нашем примере выбран алфавитный порядок букв слова

рубль. Таким образом, в зашифрованном сообщении сначала будут записаны буквы третьего столбца, затем четвертого, первого, второго и, наконец, пятого. Зашифрованное сообщение будет выглядеть так:

“одершрйтэфвптрнаиесы’’.

В общем случае перестановочный шифр порядка p переставляет блоки символов (столбцы) согласно фиксированной перестановке. Одним из удобных способов получить перестановку есть описанный выше с помощью ключевого слова. Существует $p!$ перестановок p символов или, другими словами, существуют $p!$ возможных ключей.

4. Шифры подстановки

Одними из древнейших являются *шифры подстановки.*

4.1. Шифр Цезаря. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки. При шифровании этим способом каждая буква заменяется другой, отстоящей от нее в алфавите на фиксированное число позиций k, которое и служит ключом данного шифра. Например, пусть $k = 3$. Тогда схема подстановки такова:

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

Например, текст “шифр цезаря’’ перекодируется в текст

“ъмчу щзлгув”:

25	10	21	17		23	6	9	1	17	31
ш	и	ф	р		ц	е	з	а	р	я
↓	↓	↓	↓		↓	↓	↓	↓	↓	↓
ъ	м	ч	у		щ	з	л	г	у	в
28	13	24	20		26	9	12	4	20	3

Если сопоставить каждой букве алфавита ее порядковый номер, то шифрование и дешифрование методом Цезаря можно выразить формулами:

$$y = \begin{cases} x + k, & \text{если } x + k \le n, \\ x + k - n, & \text{если } x + k > n, \end{cases}$$
$$x = \begin{cases} y - k, & \text{если } y - k \ge 0, \\ n + y - k, & \text{если } y - k < 0, \end{cases}$$

где x — символ исходного текста, y — символ шифрованного текста, n — мощность алфавита, а k — ключ.

4.2. Шифр масонов (pigpen cipher). Время, когда стали пользоваться *кодом масонов*, определить достаточно сложно. Известно, впрочем, что руководители масонских лож применяли его в переписке между собой уже в XVIII столетиии. При использовании этого шифра буквы латинского алфавита делятся на пары, которые заключаются в графические области:

Рис. 5. Ключ к шифру масонов

При шифровании первая буква каждой пары заменяется на границу соответствующей области. Например буква “e”

заменяется на “⌊_”. Вторая буква каждой пары заменяется на границу соответствующей области с добавлением символа “·”. Например, буква “f” заменяется на “⌊· ”. Примером сообщения, зашифрованного этим методом, является:

Рис. 6. Тайное масонское послание

5. Шифр Виженера

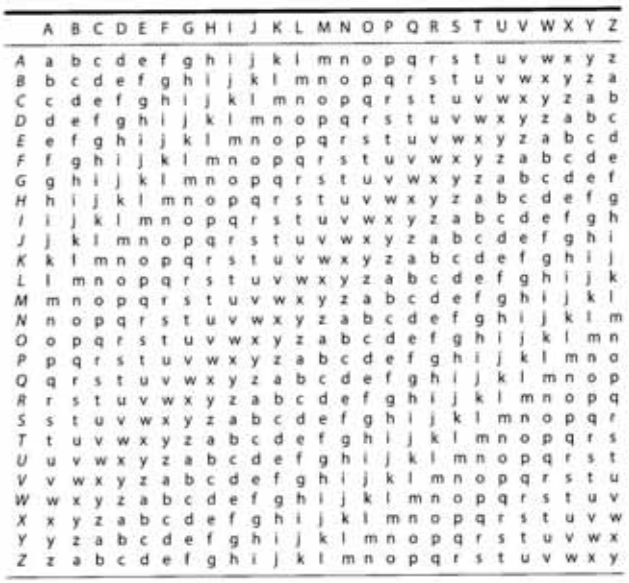
Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Впервые этот метод описал Джованни-Баттиста Беллазо в 1553 году, однако в XIX веке получил имя Блеза Виженера, швейцарского дипломата. Метод является недоступным для простых методов криптоанализа.

Ключом к шифру является фиксированное слово, буквы которого определяют сдвиги в исходном тексте. Для удобства можно использовать таблицу, которая также называется *tabula recta* (см. рис. 7).

В первой строке таблицы записан латинский алфавит. Каждая последующая строка таблицы получена из предыдущей сдвигом на одну позицию вправо.

Идею шифрования покажем на примере ключевого слова “`code`” и исходного текста “`vigenere cipher`”. Прежде всего составляем строку для замены, используя необходимое количество раз ключевое слово:

“`vigenere cipher`”
“`codecode codeco`”



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Рис. 7. Tabula recta для шифра Виженера

Теперь каждая буква исходного текста шифруется буквой из tabula recta по такому правилу: если буквой исходного текста является α, а соответствующей буквой строки ключей является β, то буквой в шифрованном тексте является та, которая стоит в tabula recta на позиции (α, β). Например, первой букве исходного текста “`v`” отвечает буква “`c`” в строке ключей. Поэтому “`v`” шифруется буквой, стоящей на пересечении столбца “`v`” и строки “`c`” в tabula recta, то есть “`x`”. Аналогично, вторая буква “`i`” шифруется буквой на пересечении столбца “`i`” и строки “`o`”, то есть “`w`”. Сообщение `vigenere cipher`” буде зашифровано в

“`xwjipsui ewslgf`”.

Обратите внимание, что буква “`e`” встречается в исходном тексте 4 раза. При этом символы, в которые она шифруется, предсказать заранее невозможно (они зависят от самого текста). В нашем примере шифрами буквы “`e`” были:

“i”, “s”, “i” и “g”.

Шифром Виженера пользовалась одна из противоборствующих сторон во время гражданской войны в США. Ключами служили последовательности “Manchester Bluff”, “Complete Victory” и “Come Retribution”.

6. Шифр Вернама

Устойчивость шифра Виженера возрастает при увеличении длины ключа. Если, например, длина ключа равна длине сообщения, а символы ключа абсолютно случайны, то и шифрованный текст не будет иметь никакой структуры, которую могли бы использовать враги для дешифрации.

Описанный специальный вариант шифра Виженера, называемый *шифром одноразового блокнота*, назван по далекой аналогии с блокнотом, каждая страница которого исписана буквами, случайно выбранными из алфавита. После первого же использования любой “страницы блокнота”, она удаляется навсегда из блокнота.

Описанная схема шифрования изобретена в 1917 году сотрудниками AT&T Мейджором Моборном и Гильбертом Вернамом. С тех пор она часто называется *шифром Вернама*. Шифр Вернама является единственной системой шифрования, для которой доказана абсолютная криптографическая устойчивость (это сделал Клод Шеннон в 1949 году). Других шифров с этим свойством не существует. Это по сути означает, что шифр Вернама является самой безопасной криптосистемой из всех возможных. При этом условия, которым должен удовлетворять ключ, настолько сложны, что практическое использование шифра Вернама становится трудно осуществимым. Поэтому он используется только для передачи сообщений наивысшей секретности.

7. Шифр Плейфера

Первое описание шифра Плейфера было зарегистрировано в документе, подписанном Чарльзом Уитстоном 26 марта 1854. Министерство иностранных дел Великобритании отклонило этот документ из-за сложности его восприятия. Описывая простоту метода, Уитстон сказал, что три из четырех мальчиков в соседней школе овладеют этим шифром за пятнадцать минут, заместитель министра иностранных дел ответил: “Это очень возможно, но вы никогда не научите этому наших дипломатов.”

Шифр назван именем лорда Плейфера, который внедрил данный шифр в государственные службы Великобритании. В тактических целях использовался британскими вооруженными силами во второй англо-бурской войне и в первой мировой войне, а также австралийцами и немцами во время второй мировой войны.

Шифр определяется специальной матрицей, называемой *таблицей Плейфера*. Один из возможных примеров приведен ниже:

8	J	E	Q	D	N	5	O
P	U	3	A	R	F	L	W
4	V	C	2	T	M	B	I
K	7	Z	S	G	X	H	Y

Таблица 4×8 образована 26 буквами латинского алфавита, дополненными цифрами 2, 3, 4, 5, 7, 8.

Предположим, что необходимо зашифровать сообщение “LET US MEET AT NOON”. Сначала все буквы разбиваются на пары: “LE TU SM EE TA TN OO N”. Первую пару одинаковых букв разбиваем символом “X”, а все последующие буквы объединяем в пары: “LE TU SM EX ET AT NO ON”. Обратите внимание, что пара “OO” теперь распалась сама по себе. Если бы в новой последовательности оставались пары, составленные из одинаковых букв, то необходимо было

бы повторить то же действие: разбить первую такую пару символом “X”, а все последующие буквы объединить в пары. Это действие необходимо повторять до тех пор, пока пар из одинаковых букв не останется.

В нашем примере пар из одинаковых букв не осталось уже после первого применения указанного действия.

Вполне могло бы так случиться, что последовательность пар заканчивалась одиночной буквой. В этом случае его необходимо было бы дополнить символом “X”.

Теперь шифрование происходит по парам с учетом следующих правил. Назовем буквы из одной пары партнерами.

1. Если обе буквы в паре находятся в одной строке таблицы Плейфера, то заменить каждую из них буквой, следующей непосредственно за ней в этой строке. Если одна из букв пары является последней в строке, то заменить ее на первую букву этой строки. Например, пара “TI” шифруется в “M4”.
2. Если обе буквы в паре находятся в одном столбце таблицы Плейфера, то заменить каждую из них буквой, следующей непосредственно за ней в этом столбце. Если одна из букв пары является последней в столбце, то заменить ее на первую букву этого столбца. Например, пара “RG” шифруется в “TD”.
3. Наконец, если партнеры в паре находятся в разных строках и столбцах таблицы Плейфера, то каждую из них заменить на букву, стоящую в той же строке, но в столбце партнера. Например, пара “LE” шифруется в “35”.

Таким образом, нужное нам сообщение кодируется в такое: “35VR X2NZ DCR2 5885”.

8. Омофонический шифр

Ранние попытки увеличивать трудность дешифровки ча-

стотным анализом состояли в уравнивании частот появления символов с помощью омофонии. В таких шифрах, буквы исходного алфавита соответствуют больше, чем одному символу из алфавита замены. Обычно, символам исходного текста наивысшей частоты отвечают больше эквивалентов, чем более редким символам. Таким образом, распределение частоты становится равномерным, сильно затрудняя частотный анализ.

Еще в XIV веке в канцелярии Папы Римского использовались шифры замены, в которых гласным буквам соответствовали несколько значковых выражений. В 1469 г. был предложен так называемый “*миланский ключ*”, в котором каждой букве ставится в соответствие несколько эквивалентов, число которых пропорционально частоте встречаемости в открытых текстах.

Более художественными, хотя не обязательно более надежными, будут омофонические шифры, которые используют придуманные (вымышленные) алфавиты (например, “Пляшущие человечки” у Артура Конан Дойла или “Золотой жук” у Эдгара По).

8.1. Книжный шифр. Это вид шифра, в котором каждый элемент открытого текста (каждая буква или слово) заменяется на указатель (например, номер страницы, строки и столбца) аналогичного элемента в дополнительном тексте, который является ключом.

Для дешифрования необходимо иметь как зашифрованный текст, так и дополнительный текст-ключ. В качестве дополнительного текста часто использовали распространённые книги, либо книги, которые с большой степенью вероятности были и у отправителя, и у адресата.

Прославленный советский разведчик Рихард Зорге с успехом использовал книжный шифр, японцы не смогли прочесть шифровки даже после ареста всех членов его аген-

турной сети.

Книжный шифр упомянут в романе Ю. Семенова “Приказано выжить” и показан в начале фильма “*Семнадцать мгновений весны*”.

Рис. 8.
Шифрограмма

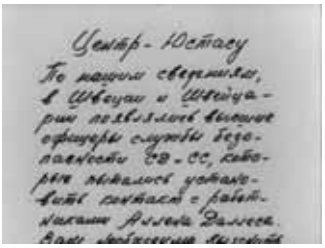


Рис. 9.
Расшифровка

Книжный шифр не считается надежным. Один из известных примеров относится к началу 20-ых годов XX века, когда Уильям Фридман (руководитель отдела секретных сообщений, США) и его жене Элизабет (главный дешифровщик отдела) смогли расшифровать код, используемый немцами и индийцами в переписке по закупке оружия для борьбы против англичан. Хотя в переписке использовался сложный книжный шифр на базе устаревшего (практически недоступного) словаря, корреспонденты подчас использовали несколько раз одно и то же указание страниц и строк для одной и той же буквы. Это и позволило Фридманам расшифровать сообщения с помощью статистических методов.

9. Электро-механическая шифровальная машина Энигма

В 1918 году немецкий изобретатель Артур Шербиус получил патент на шифровальную машину, которая впоследствии стала известна под именем *Энигма* (в переводе на русский язык “Энигма” — это “загадка”). Впрочем, право на ее изобретение мог бы оспорить голландец Гуго Кох

де Дельфт, предполагавший использовать шифровальную машину в гражданских целях.

Компания Шербиуса “Шифровальные машины” производила Энигму в течение 10 лет, но, не получив достаточного коммерческого успеха, в 1934 г. была ликвидирована и передала свои активы другой фирме. По иронии судьбы вскоре после этого машина были признана достаточно надежной и удобной и широко использовалась в германской армии, ВМС и ВВС. Энигма использовалась в коммерческих целях, а также в военных и государственных службах во многих странах мира, но наибольшее распространение получила в нацистской Германии во время Второй мировой войны.

Рис. 10. Вид машины Энигма

Главное преимущество Энигмы — безопасность. Даже заполучив машину, противник не сможет ею воспользоваться: она надежно хранит свои тайны, а регулярно меняющийся ключ превращает конкретный экземпляр машины, случайно попавший в руки противника, в бесполезный музейный экспонат.

Энигма — это портативная шифровальная машина, точнее, это — целое семейство электромеханических роторных машин, применявшихся с 20-х годов XX века. Вид машины изображен на рис. 10.

Энигма состоит из комбинации механических и электрических систем. Механическая часть включает в себя клавиатуру и набор вращающихся дисков (роторов), похожих на диски Джефферсона.

Каждый ротор Энигмы имеет 26 контактов с лицевой стороны и 26 с обратной. Контакты соединены попарно: один на лицевой стороне и один на обратной. Соединение парами является абсолютно нерегулярным и определяет подстановочный код этого ротора. Если бы машина имела один ротор, то она бы осуществляла простое подстановочное шифрование.

Однако наличие трех роторов и последовательное применение подстановочного кода на каждом из них резко усложняло процесс дешифровки. Роторы были абсолютно взаимозаменяемы, поэтому любая последовательность прохождения сигнала через роторы была возможной. Последовательность определялась оператором заранее и это увеличивало количество возможных шифров в 6 раз. Перед началом работы роторы проворачивались таким образом, чтобы установилось кодовое слово.

В момент нажатия клавиши происходило шифрование очередного знака открытого текста. При этом электрический импульс поступал с клавиатуры и проходил через систему роторов, после чего первый ротор поворачивался на один шаг. Движение роторов происходило как в счетчике электроэнергии: после полного оборота первого ротора на один шаг поворачивался второй ротор; после полного поворота второго ротора сдвигался на один шаг третий ротор.

Четвертый диск, называемый рефлектором, был неподвижен и имел контакты только на лицевой стороне. Контакты рефлектора также соединены попарно, поэтому приходящий с роторов сигнал коммутировался рефлектором и возвращался через роторы по абсолютно другому пути. Обратный сигнал от роторов заканчивался на панели из 26

ламп, которые служили индикаторами результата шифрования.

На самом деле Энигма была еще сложнее за счет так называемых *мостов* и *колец*. Мосты соединяли буквы попарно, что позволяло подменять нажатую клавишу другой еще до попадания сигнала на роторы. Кольцо же соединялось с одним из роторов и определяло условие, при котором следующий ротор поворачивался на одну позицию до попадания на него сигнала с предыдущего ротора.

Упрощенная схема работы машины при нажатии клавиши “Z” изображена на рис. 11.

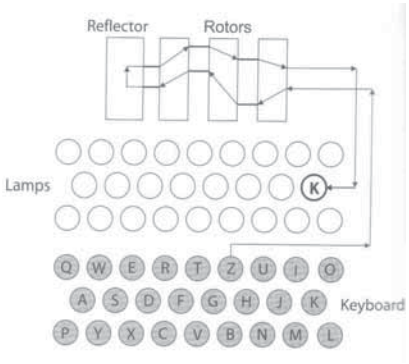


Рис. 11. Схема машины Энигма

Нажатие клавиши “Z” замыкает электрический контур; электрический сигнал от клавиши “Z” проходит через три ротора и поступает на рефлектор, откуда возвращается на роторы, направляющие его (в данном примере) к лампе с буквой “K”, которая и служит шифром для буквы “Z”.

Количество шифров, которые может генерировать трехроторная Энигма, превосходит 15×10^{22}!

Во время второй мировой войны Энигма широко использовалась в германской армии. Аппарат был достаточно портативным (размером с пишущую машинку), работал от батареи, имел деревянный футляр. Недостатком было то, что

машина не печатала шифртекст (впрочем, в более поздних модификации это неудобство было устранено). Кроме того, для быстрой работы требовались три или даже четыре человека: для чтения и набора текста сообщения, диктовки высвечивающихся букв шифртекста и их записи.