Агафонова Ирина Витальевна

ЭВОЛЮЦИЯ ШИФРОВ ЗАМЕНЫ: ИДЕИ И МЕХАНИЗМЫ. ЧАСТЬ 2. МНОГОАЛФАВИТНЫЕ СИСТЕМЫ

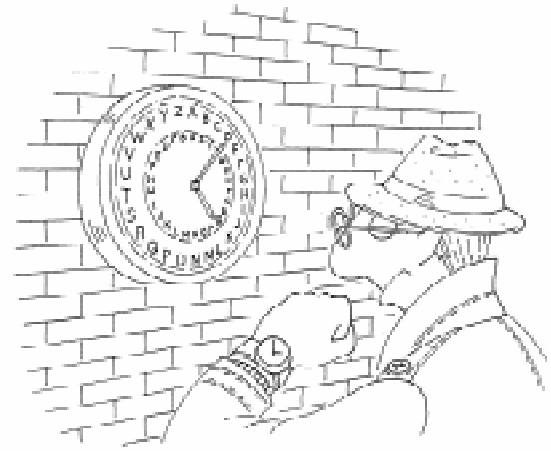
ШИФР АЛЬБЕРТИ (1466)

Частотный анализ сильно затрудняется, когда используется больше одного алфавита. Первый прорыв такого рода связан с именем Леона Альберти. Гордый автор назвал его шифром, «достойным королей».

Для шифрования Альберти использовал устройство, которое сейчас называют его именем – шифровальный диск Альберти. Это, собственно, два диска с общей осью, неподвижный внешний и подвижный внутренний. На рисунке 1 изображена модель диска Альберти, соответствующая современному английскому алфавиту. Круг разбит на 26 секторов по числу букв алфавита, изображенных как на неподвижном, так и на подвижном диске.

На внешнем диске мы будем отыскивать по очереди буквы, которые хотим зашифровать, они удобно расположены по алфавиту.

В начале шифрования внутренний диск поворачивают так, что буква *A* на внешнем диске совмещается с заранее оговоренной буквой внутреннего диска (например, с буквой *n*, как на рисунке 1). После этого очередная буква исходного текста, найденная во внешнем круге, заменяется стоящей под ней буквой из внутреннего круга. Алфавит замены, расположенный на внутреннем диске, в данном случае начинается с *n* и совпадает с



...алфавит внутреннего диска ориентирован против часовой стрелки...

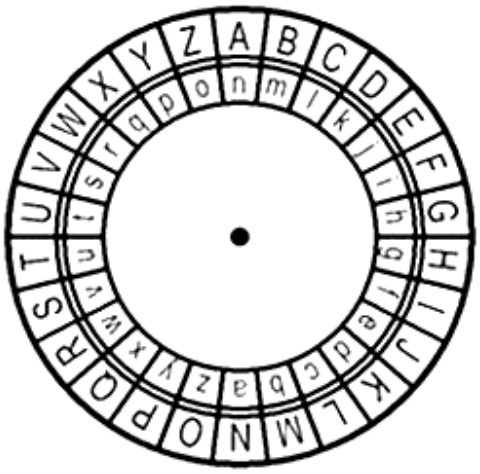


Рисунок 1.

Таблица 1. Двухалфавитная замена

буква	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
1-й код	n	m	l	k	j	i	h	g	f	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o
2-й код	e	d	c	b	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f

первым кодом, приведенным ниже в таблице 1.

То, что алфавит внутреннего диска ориентирован против часовой стрелки, не является обязательным. Алфавиты могут быть одинаково направлены, и, вообще, буквы внутреннего алфавита могут идти в любом порядке, как это и сделано у Альберти. Его исторический диск схематично представлен на рисунке 2.

На этом диске круг разбит на 24 сектора, внешний диск помечен 21 основными буквами и цифрами от 1 до 3, внутренний – всеми 23 буквами перемешанного латинского алфавита и *et* (союз «и»). Цифры 1, 2, 3 в различных сочетаниях Альберти предназначил для сокращенного обозначения каких-либо часто встречающихся слов или фраз по выбору переписывающихся.

Как видим, диск – это механическое устройство для осуществления простой замены. Изобретение такого устройства еще не объясняет, почему Альберти признают отцом западноевропейской криптологии. Главная заслуга Альберти – использование не одного, а нескольких алфавитов, что затрудняет частотный анализ. Переключение с одного алфавита на другой Альберти предлагал производить через каждые 3–4 слова. Это делается поворотом внутреннего диска в ту или другую сторону на определенное число делений. Сигналом такого переключения для получателя было появление в шифрованном тексте заглавной буквы. Без этой причины заглавные буквы в тексте не допускались. Первоначально Альберти использовал два алфавита, затем больше.

Мы для примера возьмем 2 разных 26-буквенных алфавита внутреннего диска, один будет начинаться с буквы *n*, другой – с буквы *e*. Будем переключаться с одного на другой после каждой буквы.

В [1] мы пользовались только 1-м алфавитом, и тогда сообщение *«secret»* кодировалось как *«vjlwju»*. Теперь это же сообщение закодируется как *«valnjl»*. Видим, что первая и вторая буква *e* шифруются разными знаками, а разные буквы *c* и *t* получили одинаковый код. Простой частотный анализ не справится с расшифровкой такого текста.

Можно сказать, что набор из двух алфавитов определяется словом *«ne»,* и, вообще, набор и последовательность алфа-

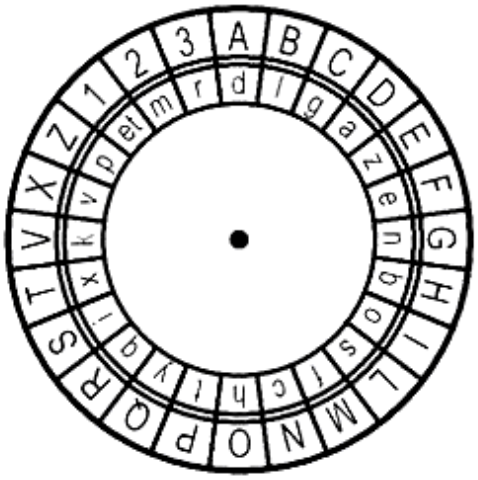


Рисунок 2.

...набор из двух алфавитов определяется словом «ne»...

Таблица 2. Многоалфавитная замена

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

витов определяются некоторым ключевым словом, которое знают отправитель и получатель шифрованного сообщения.

Чтобы использовать шифр Альберти, не обязательно изготавливать диск, хотя это полезное и интересное упражнение. Можно составить таблицу всех возможных алфавитов, заметив, что разные алфавиты сдвинуты относительно друг друга на определенное число позиций. Мы составим такую таблицу. Для сравнения с последующими шифрами нам удобно взять диск, изображенный на рисунке 3 , где внутренний алфавит совпадает с внешним.

Строчки таблицы будут соответствовать 26-ти алфавитам замены, получаемым при сдвиге внутреннего от начального положения *A–a* на 0, 1, 2, ..., 25 делений по часовой стрелке. Первая строка, таким образом, содержит основной алфавит. Таблица 2 состоит из 26 шифров Цезаря (первый – тривиальный).

Пусть ключевым будет слово *«metro»*. Тогда первый алфавит замены берется из строки с первой буквой *m*, второй – из строки с первой буквой *e*, и так далее.

Эта таблица встретится нам еще не раз.

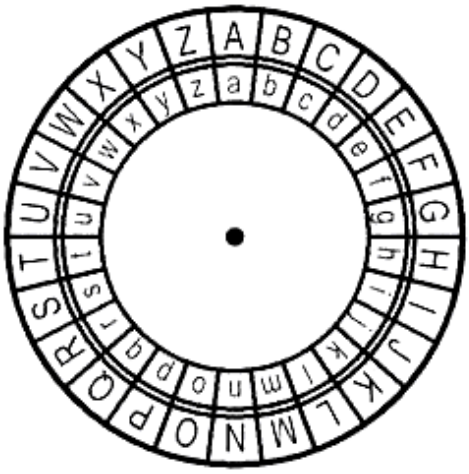


Рисунок 3.

...представим сложение номеров букв как сложение самих букв...

ТАБЛИЦА АББАТА ТРИТЕМИУСА (1508)

Этот шифр использует столько разных алфавитов, сколько имеется букв в алфавите конкретного языка.

Для описания этого шифра часто нумеруют буквы, чтобы складывать их номера, но мы поступим иначе, сближая описания шифра Тритемиуса и других рассматриваемых шифров. Мы представим сложение номеров букв как сложение самих букв по очевидному правилу: вместо того, чтобы сказать, что суммой 12-й и 3-й буквы является 15-я буква, мы скажем, что $m + d = p$. (Нумерацию букв нам удобно начать с 0). Ограничение для номеров букв – от 0 до 25 – снимается, если договориться, что 26-я буква – это снова *a*, 27-я – это буква *b*, и так далее по алфавиту.

Составим «таблицу сложения» для букв. Она в точности совпадает с таблицей 2.

Как производится сложение двух букв? Отыщем одну из этих букв в первом столбце и отметим соответствующую строку, а другую – в первой строке, отметив столбец. Суммой двух букв считаем букву, стоящую на пересечении отмеченных строки и столбца, так что, например, $m + p = b$. Буква *a* тогда играет роль нуля: ее прибавление к другой букве не изменяет эту букву; в частности, $a + a = a$.

Такая квадратная таблица, «tabula recta», впервые описана в сочинении Тритемиуса «Шесть книг о полиграфии». (В подлинной таблице Тритемиуса буквы *j* и *v* были исключены). Тритемиус отводил первую строку для кодирования первой буквы сообщения, вторую для второй, и так до 24-й, после чего возвращался к 1-й строке.

Зашифруем по таблице 2, например, первые слова студенческого гимна «Gaudeamus igitur» (без учета пробела). Шифр каждой буквы стоит в ее столбце: для первой буквы в первой строке, для второй во 2-й, и так далее. Получаем код, приведенный в таблице 3.

Шифр Тритемиуса – периодический, его алфавиты повторяются через определенное число замен (в нашем примере – через 26). Именно Тритемиус предложил менять шифр после каждой буквы, что еще больше защищает тайну переписки. Перемешивание букв алфавита Тритемиус не применял.

ШИФР БЕЛАЗО (1553)

Если у Тритемиуса строки таблицы используются по порядку их номеров, то Джованни Белазо предложил определять порядок применяемых алфавитов с помощью специально выбранного слова – *пароля*. Сейчас такое слово обычно называют *лозунгом* или *ключом*. Мы уже затронули идею ключевого слова, когда обсуждали шифр Альберти. В этой статье термины «лозунг» и «ключ» будем считать синонимами и шифры с использованием ключа называть *лозунговыми*.

Рассмотрим пример применения лозунгового шифра.

Таблица 3. Пример многоалфавитной замены

текст	g	a	u	d	e	a	m	u	s	i	g	i	t	u	r
код	g	b	x	g	i	f	s	b	a	r	q	t	f	h	f

Таблица 4. Пример многоалфавитной лозунговой замены

лозунг	e	n	i	g	m	a	e	n	i	g	m	a	e	n	i
текст	g	a	u	d	e	a	m	u	s	i	g	i	t	u	r
код	k	n	c	j	q	f	q	h	a	o	s	i	x	h	z

Выберем лозунг *«enigma»* (загадка). Этот лозунг надпишем над сообщением, которое хотим зашифровать. Лозунг намного короче сообщения, и его повторяют многократно. Шифром буквы сообщения будет сумма этой буквы и стоящей над ней буквы лозунга.

Это правило применительно к таблице 2 означает, что шифр каждой буквы берется в ее столбце и в строке, начинающейся с очередной буквы лозунга.

(Такой способ шифрования, когда символы исходного текста складываются по одному с символами некоторой последовательности, в современной криптографии называют *гаммированием*, а саму шифрующую последовательность – *гаммой*. В шифре Белазо гамма состоит из многократно повторенных одинаковых лозунгов.)

Теперь текст «Gaudeamus igitur» шифруется так (таблица 4).

Тот, кто знает ключ, легко расшифрует закодированное сообщение. (Подумайте, как).

Опишем простое механическое устройство, реализующее лозунговую замену. Оно носит название «линейка Сен-Сира», так как появилось во французской военной академии Сен-Сир. Было это уже в XIX веке, когда искусство шифрования начали изучать в военных школах.

Линейка состояла из неподвижной шкалы с нанесенным на нее алфавитом, и подвижной шкалы с тем же самым алфавитом, повторенным дважды. Подвижная шкала вставлялась в прорези неподвижной и могла там свободно перемещаться (рисунок 4).

Для кодирования первой буквы текста полоски приводились в положение, когда первая буква лозунга (на нашем рисунке это *e*) оказывалась под буквой *a*. Тогда под первой буквой текста окажется ее код. На рисунке кодом буквы *g* будет буква *k*. Для второй буквы текста требуется передвинуть полоску так, чтобы под *a* оказалась вторая буква лозунга, и так далее.

Линейка была достаточно широко распространена, так как изготовить ее совсем просто.

ШИФР ДЕ ЛА ПОРТА (1563)

Книга «О тайной переписке» известного ученого Джованни Батиста де ла Порта из Неаполя – это и научный труд, и учебник по криптографии, в ней содержится обзор и классификация известных методов скрытого письма и собственные предложения автора. Из идей де ла Порта нас интересует перемешивание букв в лозунговом многоалфавитном шифре.

Перемешивание здесь производится лишь один раз: изменяется последовательность букв в первой строке таблицы 8. Начнем, например, первую строку со слова cryptogram (все буквы разные), а затем разместим остальные буквы в алфавитном порядке.

Каждую следующую строку, как и в таблице 2, будем получать циклическим сдвигом предыдущей строки на одну позицию влево.

Нам понадобится добавить к таблице заголовочные строку и столбец с исходным алфавитом. В таблице 2 в них не было нужды, они совпадали с первой строкой и первым столбцом (таблица 5).

Рисунок 4.

Таблица 5. Многоалфавитный шифр с перемешиванием
(приведены первые и последние строки таблицы)

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

По этой таблице, взяв прежний лозунг «enigma», зашифруем слово «abbacy». Код представлен в таблице 6.

ШИФР ВИЖЕНЕРА (1586)

Общепринятым для шифров с периодической гаммой, использующих таблицы 2 или 5, является название «шифр Виженера» (иногда Вижинера или Вижанэра), и сами эти таблицы называют таблицами Виженера. (Чаще всего при этом имеется в виду неперемешанная таблица 2). Между тем, как мы уже видели, эти шифры не изобретены Виженером. В работе «Трактат о шифрах» Блез де Виженер свел вместе идеи таблицы (Тритемиус), ключа (Белазо) и перемешивания (Порта). Собственно, Виженеру принадлежит другая идея: применить в качестве составляющей ключа сам текст, который предстоит зашифровать.

Такой подход, для которого сейчас применяют термин «автоключ» или «самоключ», еще до Виженера предложил великий Джироламо Кардано – физик, математик, философ, врач, в честь которого, в частности, назван карданный механизм. Но революционная идея автоключа в том виде, в каком она была впервые предложена Кардано, оказалась непрактичной. А предлагалось следующее.

...идея: применить в качестве составляющей ключа сам текст, который предстоит зашифровать.

Сохранялось разбиение исходного текста на слова, и ключом для зашифровки каждого слова длины *N* служили первые *N* букв исходного текста. Например, зашифруем таким образом по таблице 2 начало текста «We start the new project». Получим код, приведенный в таблице 7.

Минусы этого шифра нетрудно обнаружить. Во-первых, получатель должен знать первое слово текста. Во-вторых, и всякий другой, узнав первое слово, расшифрует текст. В третьих, первые буквы всех слов кодируются одним и тем же алфавитом таблицы 8, а это позволяет применять частотный анализ.

Усовершенствование Виженера было в том, чтобы иметь короткий первичный ключ, который будет служить началом гаммы, и дополнить его самим исходным текстом. Пробелы между словами не нужны. Взяв, например, для текста «We start the new project» первичный ключ *«enigma»*, получаем, используя таблицу 2, код, начало которого приведено в таблице 8.

Таблица 6. Пример шифрования по таблице 5

лозунг	e	n	i	g	m	a
текст	a	b	b	a	c	y
код	t	f	m	g	h	x

Таблица 7. Пример использования автоключа Кардано

лозунг	w	e		w	e	s	t	a		w	e	s		w	e	s
текст	w	e		s	t	a	r	t		t	h	e		n	e	w
код	s	i		o	x	n	k	t		p	l	w		j	i	o

Таблица 8. Пример использования автоключа Виженера

лозунг	e	n	i	g	m	a	w	e	s	t	a	r	t	t	h	e
текст	w	e	s	t	a	r	t	t	h	e	n	e	w	p	r	o
код	a	r	a	z	m	r	p	x	z	x	n	v	p	i	y	s

Шифр Виженера как с автоключом, так и с обычным ключом уже настолько сложен для взлома, что был провозглашен невзламываемым и действительно оставался таковым почти триста лет, до середины XIX века. Вскрытие его связано с именами английского ученого Чарльза Бэббиджа и прусского офицера Фридриха Казиски. Первое, что необходимо для прочтения зашифрованного текста, – это исследование повторяющихся сочетаний букв, с помощью чего определяют длину ключа. Затем применяют вариант частотного анализа.

ШИФРУЮЩИЙ ЦИЛИНДР ДЖЕФФЕРСОНА (1790)

Томас Джефферсон, будущий президент США, предложил осуществлять многоалфавитную замену с помощью устройства, состоящего из дисков, по ободу которых написаны перемешанные буквы алфавита. Дисков обычно от 20 до 40, они надеты на общую ось и прилегают друг к другу вплотную, образуя цилиндр. Рисунок 5 – упрощенный, на нем изображены лишь два соседних диска, причем они отодвинуты друг от друга, а часть букв заменена точками.

Диски можно вращать и выстраивать буквы с разных дисков в линии вдоль оси цилиндра. На рисунке 5 буквы *u* и *z* находятся на одной горизонтальной линии, буквы *d* и *o* на другой, а всего линий 26, по числу букв алфавита, нанесенных на диски.

Если дисков, например, 40, то текст, который надо зашифровать, разбивают на блоки по 40 букв. Шифровальщик вращением дисков выстраивает первые 40 букв текста в горизонтальную линию. Кодом этого текста будет 40 букв на другой линии, можно выбрать любую линию из оставшихся 25-и. Так же шифруется и следующий 40-буквенный блок. Для расшифровки блока из 40 знаков эти знаки набирают в одну линию, а затем, просматривая оставшиеся линии, находят среди них ту, в которой содержится осмысленный текст.

Диски у отправителя и получателя, конечно, должны быть одинаково надписаны, и порядок их вдоль оси тоже должен совпадать. Если заранее договориться и регулярно по условленному правилу менять порядок дисков на том и на другом цилиндре, то взлом шифра, и без того непростой, еще усложнится.

ШИФРОВАЛЬНАЯ МАШИНА «ЭНИГМА» (1923)

С появлением в XIX веке телеграфной связи и радиосвязи в XX веке перехват сообщений стал обычным явлением. От систем шифрования потребовалась еще

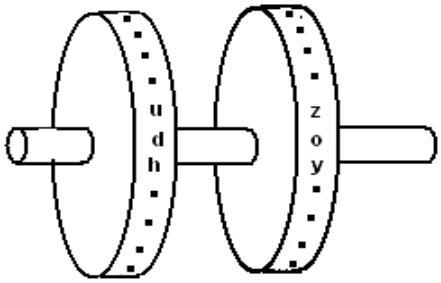


Рисунок 5.

более высокая стойкость ко взлому. В то же время усложнение шифров и возросшие объемы переписки сильно повышали риск возникновения ошибок в ходе шифрования.

После первой мировой войны стало ясно, что операции шифрования и расшифровки надо предоставить машинам. И такие машины появились.

В начале 20-х годов в Германии появились первые машины многоалфавитной замены с очень большим числом используемых алфавитов. Знаменитая «Энигма» была создана Артуром Шербиусом, совладельцем одной немецкой инженерной компании.

Что такое была шифровальная машина «Энигма»? Основу ее составляли роторы, обычно их было три или четыре.

Ротор, или контактное колесо, – это диск из твердой резины или пластмассы, полый внутри. На каждой стороне диска расположены по 26 электрических контактов. Каждый контакт на одной стороне соединен внутренним проводом с каким-то контактом на другой стороне. Контакты соответствуют 26 буквам латинского алфавита, и такое соединение механически осуществляло шифр простой замены. Электрический импульс, поступающий на контакт одной стороны, передается на соединенный с ним контакт другой стороны.

На рисунке 6 изображены две стороны одного ротора и два контактных провода из 26-ти. Если на правую сторону поступает импульс, то он передается на контакт левой стороны, то есть буква *a* шифруется как *d*, а буква *b* – как *z*. Однако если ротор вместе с контактными проводами будет повернут, скажем, на одно деление, то имена контактов изменятся. Теперь первый провод будет переводить не букву *a* в *d*, а букву *b* в *e*, второй – не букву *b* в *z*, а букву *c* в *a*, и то же произойдет со всеми заменами. Мы получаем уже другой алфавит замены. При сдвиге еще на деление – третий, а всего таким образом мы можем получить 26 различных шифров замены. При желании их можно записать в таблицу размером 26×26, такую же, как таблицы 2 и 5, где первая строка будет определяться внутренней распайкой ротора.

Шифров замены становится гораздо больше, чем 26, если соединить несколько роторов. Трехроторная машина порождает уже 26×26×26 алфавитов.

Шифровальная машина «Энигма», кроме подвижных дисков – роторов, использует еще отражатель – неподвижный диск. Отражатель имел контакты только на одной стороне, и эти 26 контактов имели внутренние попарные соединения, образуя 13 пар. Был и еще один неподвижный диск – колесо ввода. Оно осуществляло связь между первым ротором и устройствами ввода-вывода: клавиатурой, на которой набирался текст, и панелью с лампочками, на которой подсвечивалась буква, полученная в результате шифрования.

На ободы роторов нанесены буквы алфавита, что позволяет определять и устанавливать взаимное расположение роторов.

Схематично устройство «Энигмы» с тремя роторами R1, R2, R3, колесом ввода K и отражателем U (по-немецки он назывался Umkehrwalse – «возвращающий диск») можно представить диаграммой на рисунке 7, на которой диски изображены со стороны обода.

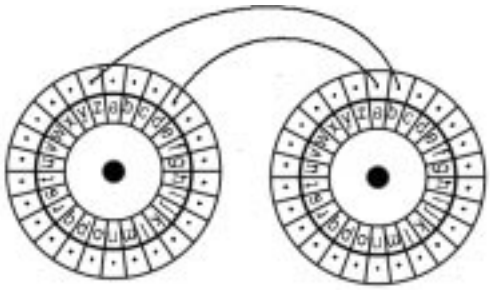


Рисунок 6.

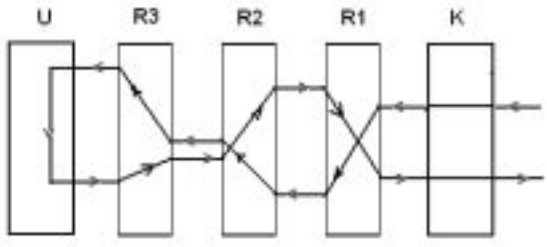


Рисунок 7.

Смена шифроалфавитов осуществлялась после ввода каждой буквы по принципу поворота колес счетчика, то есть следующим образом:

– ротор R1 поворачивался на одно деление;

– если первый ротор совершал полный круг, то ротор R2 поворачивался на одно деление;

– если второй ротор совершал полный круг, то ротор R3 поворачивался на одно деление.

В силу одной технической особенности вместе со сдвигом ротора R3 должен был сдвигаться и R2, так что разных шифров замены было на самом деле $26 \times 25 \times 26 = 16900$.

В «Энигме» получалась симметричная картина: если буква *а* при шифровании переходила в букву *х*, то и буква *х* при такой же установке колес переходила в *а*. Так что для расшифровки надо было установить машину в исходное положение и набирать закодированный текст. Загорающиеся лампочки восстанавливали посланное сообщение.

Ни одна буква при таком шифровании не могла оказаться своим собственным кодом, и эта всем известная особенность сыграла свою роль в том, что шифры «Энигмы» были взломаны во время второй мировой войны. В работе по взлому использовались результаты польских криптологов, переданные в 1939 г. англичанам. Работу возглавлял блестящий английский математик Алан Тьюринг, и вел ее целый научный центр – Британская школа кодов и шифров, расположенная в Блетчли Парк (Bletchley Park) в Оксфордшире. История с шифрами «Энигмы» заслуживает отдельного описания. Этой истории посвящено множество материалов и в их числе книга [2].

ШИФРЫ ЗАМЕНЫ В КОМПЬЮТЕРНУЮ ЭПОХУ

В эпоху, когда и шифрование, и взлом шифров осуществляют быстродействующие вычислительные машины, к системам шифрования предъявляется требование высокой стойкости даже при известном взломщику алгоритме шифрования. От таких систем требуется также экономичность, эффективность, доступность. Всем этим требованиям удовлетворяют системы, принимаемые в качестве стандартов шифрования.

В США для передачи секретных сообщений широко распространен стандарт DES (Data Encryption Standard). В России принят ГОСТ 28147-89. Оба эти стандарта блочные, то есть сообщение разбивается на блоки определенной длины, в DES и ГОСТ это 64 бита, и каждый блок преобразуется в блок шифрованного текста той же длины. (Кроме блочных, существуют поточные системы, когда шифруется каждый поступающий символ).

Стандарты DES и ГОСТ основаны на замене с секретным ключом. Длина ключа в DES составляет 56 бит, в ГОСТ – 256 бит. Кроме многократных замен, стандарт DES использует перестановки, а стандарт ГОСТ – циклические сдвиги.

Литература

1. *Агафонова И.В., Дмитриева О.М.* Эволюция шифров замены. Часть 1 // Компьютерные инструменты в образовании, № 5, 2006.

2. *Лайнер Л.* Погоня за «Энигмой». Как был взломан немецкий шифр. М.: Молодая гвардия, 2004.

Агафонова Ирина Витальевна, кандидат физико-математических наук, доцент кафедры исследования операций Санкт-Петербургского государственного университета.