Озеров В В 911 гр

Введение.

В двадцатых годах прошлого века для автоматизации процесса шифрования были изобретены различные механические шифровальные устройства. Большинство из них - американская машина SIGABA (M-134), английская TYPEX, немецкая ENIGMA, японская PURPLE были роторными машинами. основе конструкции большинства таких машин лежала концепция ротора – механического колеса, используемого для выполнения подстановки. Роторная машина состоит из клавиатуры и набора связанных между собой роторов. Принцип работы таких машин основан на много алфавитной замене символов исходного текста по длинному ключу согласно версии шифра Вижинера. Остановимся подробнее на этом шифре.

Рис 1. Немецкая шифровальная роторная машина Enigma.

Система шифрования Вижинера

Система Вижинера впервые была опубликована в 1586 г. и является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени французского дипломата XVI века Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. На рисунках ниже показаны таблицы Вижинера для русского и английского алфавитов соответственно.

Таблица Вижинера используется для зашифрования и расшифрования. Таблица имеет два входа:

• верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;

• крайний левый столбец ключа.

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Пусть ключевая последовательность имеет длину r, тогда ключ r-алфавитной подстановки есть r-строка

$$\bar{\pi} = (\pi_0, \pi_1, \ldots, \pi_{r-1})$$

Система шифрования Вижинера преобразует открытый текст $\bar{x} = (x_0, x_1, \ldots, x_{n-1})$ в шифртекст $\bar{y} = (y_0, y_1, \ldots, y_{n-1})$ с помощью ключа $\bar{\pi} = (\pi_0, \pi_1, \ldots, \pi_{r-1})$ согласно правилу

$$T_\pi : \quad \bar{x} = (x_0, x_1, \ldots, x_{n-1}) \to \bar{y} = (y_0, y_1, \ldots, y_{n-1}),$$

$$(y_0, y_1, \ldots, y_{n-1}) = (\pi_0(x_0), \pi_1(x_1), \ldots, \pi_{n-1}(x_{n-1}))$$

где $\pi_i = \pi_{(i \bmod r)}$.

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

Таблица Вижинера для русского алфавита

Ключ	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
0	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	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Таблица Вижинера для английского алфавита

Рассмотрим пример получения шифр текста с помощью таблицы Вижинера. Пусть в качестве ключа выбрано слово АМБРОЗИЯ. Необходимо зашифровать сообщение ПРИЛЕТАЮ СЕДЬМОГО.

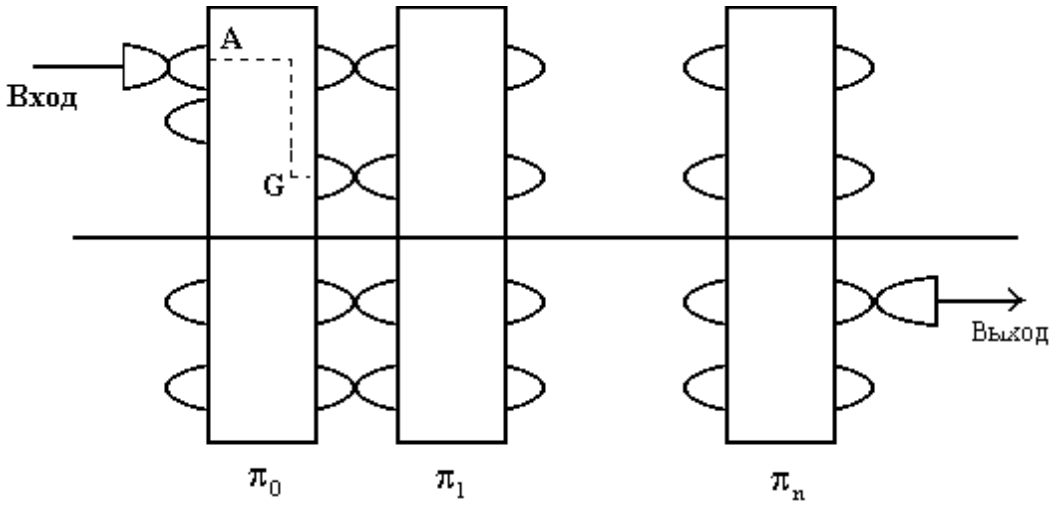
Выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением. В третью строку будем выписывать буквы шифр текста, определяемые из таблицы Вижинера.

Сообщение	П	Р	И	Л	Е	Т	А	Ю	С	Е	Д	Ь	М	О	Г	О
Ключ	А	М	Б	Р	О	З	И	Я	А	М	Б	Р	О	З	И	Я
Шифр текст	П	Ъ	Й	Ы	У	Щ	И	Э	С	С	Е	К	Ь	Х	Л	Н

Принцип действия роторной машины.

В 20-х годах XX века были изобретены электромеханические устройства шифрования, автоматизирующие процесс шифрования. Принцип работы таких машин основан на многоалфавитной замене символов исходного текста по длинному ключу согласно версии шифра Вижинера. Большинство из них - американская машина SIGABA (M-134), английская TYPEX, немецкая ENIGMA, японская PURPLE были роторными машинами.

Главной деталью роторной машины является ротор (или колесо) с проволочными перемычками внутри. Ротор имеет форму диска (размером с хоккейную шайбу). На каждой стороне диска расположены равномерно по окружности m электрических контактов, где m - число знаков алфавита (в случае латинского алфавита m = 26). Каждый контакт на передней стороне диска соединен с одним из контактов на задней стороне, как показано на рисунке. В результате электрический сигнал, представляющий знак, будет переставлен в соответствии с тем, как он проходит через ротор от передней стороны к задней. Например, ротор можно закоммутировать проволочными перемычками для подстановки G вместо A, U вместо B, L вместо C и т.д.



Банк роторов

При повороте ротора из одного положения в другое подстановка, которую он осуществляет в приходящем сигнале, будет изменяться. В общем случае эту подстановку можно записать в виде

$$T = C^j \square C^{-j}, \quad (15)$$

где $\square$ - подстановка, реализуемая ротором в его начальном положении; C - циклический сдвиг на одну позицию; C^j - циклический сдвиг на j позиций.

Например, если начальная подстановка ротора $\square(A) = G$ и ротор сдвигается на три позиции (j = 3) , то открытый текст D будет против того контакта ротора, который используется

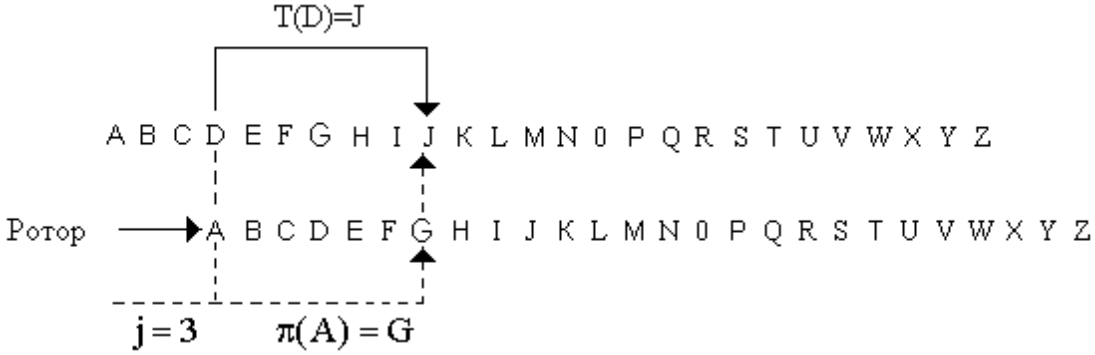


Схема формирования подстановки при сдвиге ротора (j =3)

для представления открытого текста A, а шифрованный текст J окажется против того контакта ротора, который используется для представления шифрованного текста G , и результирующая подстановка T(D) = G при j = 3. Алгебраически это записывается в виде

$$T(D) = C^3 \square C^{-3}(D) = C^3 \square (A) = C^3 (G) = J.$$

Роторы можно объединить в банк роторов таким образом, чтобы выходные контакты одного ротора касались входных контактов следующего ротора. При этом электрический импульс от нажатой клавиши с буквой исходного текста, входящий с одного конца банка роторов, будет переставляться каждым из роторов, до тех пор, пока не покинет банк.

Математически работу банка роторов можно описать в виде

$$T = C^{j_1}\pi_1 C^{-j_1} C^{j_2}\pi_2 C^{-j_2} \dots C^{j_{n-1}}\pi_{n-1} C^{j_n} C^{-j_{n-1}}\pi_n C^{-j_n} =$$
$$= C^{j_1}\pi_1 C^{j_2-j_1}\pi_2 \dots \pi_{n-1} C^{j_n-j_{n-1}}\pi_n C^{-j_n}.$$

Такой банк может реализовывать большое число подстановок, соответствующих различным комбинациям положений роторов. Для получения сильной криптографической системы расположение роторов должно меняться при переходе от знака к знаку сообщения.

Роторная машина состоит из банка роторов и механизма для изменения положения роторов с каждым зашифрованным знаком, объединенного с устройствами ввода и вывода, такими как устройство считывания с перфоленты и печатающее устройство.

Простейшее из возможных движений ротора - это движение по принципу одометра; оно использовалось в немецкой машине Enigma во время второй мировой войны. При шифровании одного знака правое крайнее колесо поворачивается на одну позицию. Когда это (и любое другое) колесо переместится на m позиций и совершит полный оборот, колесо, расположенное слева от него, передвинется на одну позицию, и процесс будет повторяться. Этот процесс проведет банк роторов сквозь все его возможные положения, прежде чем цикл повторится. Поскольку все роторы перемещаются с разными скоростями, период n-роторной машины составляет 26^n (при m = 26).

Для закона движения ротора желательны следующие характеристики:

• период должен быть большим;

• после шифрования каждого знака все роторы или большая их часть должны повернуться друг относительно друга.

Движение по принципу одометра оптимально в смысле первого требования, но совершенно неудовлетворительно в отношении второго требования. Улучшение движения по принципу одометра можно получить, если поворачивать каждый ротор более чем на одну позицию. Если смещения каждого ротора не имеют общих множителей с объемом алфавита m, то период останется максимальным.

Другое решение заключается в ограничении числа допустимых остановочных мест для каждого ротора за счет введения внешнего фиксирующего кольца, на котором

определенным способом зафиксированы места остановок. При использовании латинского алфавита можно заставить машины поворачиваться и останавливаться следующим образом. Первому колесу разрешается останавливаться в каждой из 26 позиций, второму колесу - только в 25 позициях, третьему колесу - только в 23 позициях, и так далее до шестого колеса, которому разрешается останавливаться только в 17 позициях. Период такой роторной машины теперь составляет 101 млн, а не 26^6 309 млн**,** как в случае движения по принципу одометра. Потеря в длине периода с успехом окупается полученной сложностью движения роторов. Теперь второе требование удовлетворяется довольно хорошо, поскольку каждое из колес перемещается после шифрования каждого знака и многие колеса могут двигаться друг относительно друга.

Роторная машина может быть настроена по ключу изменением любых ее переменных:

•роторов;

•порядка расположения роторов;

•числа мест остановки на колесо;

•характера движения и т.д.

Поскольку перекоммутировать роторы трудно, то обычно на практике машины обеспечивали комплектом роторов, в котором находилось больше роторов, чем можно одновременно поместить в машину. Первичная настройка по ключу производилась выбором роторов, составляющих комплект. Вторичная настройка по ключу производилась выбором порядка расположения роторов в машине и установкой параметров, управляющих движением машины. С целью затруднения расшифрования шифртекстов противником роторы ежедневно переставляли местами или заменяли. Большая часть ключа определяла начальные положения роторов ($2б^3$=17576 возможных установок) и конкретные перестановки на коммутационной доске, с помощью которой осуществлялась начальная перестановка исходного текста до его шифрования (26!= $4 \cdot 10^{26}$ возможностей).

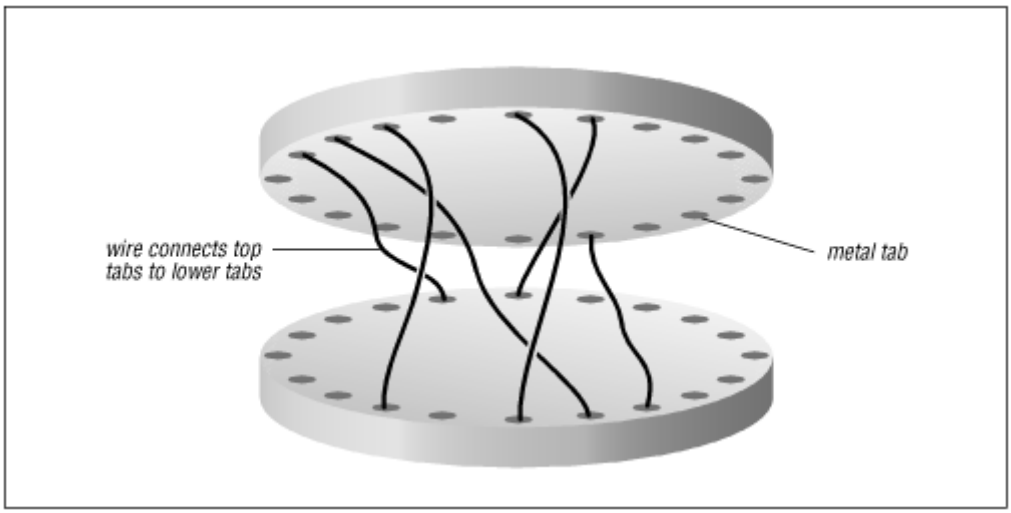
Роторные машины были самыми важными криптографическими устройствами во время второй мировой войны и доминировали по крайней мере до конца 50-х годов.

Рассмотрим подробнее одну из них, немецкую Enimgy.

Шифромальная система Enigma.

Шифровальное устройство Enigma использовалось немцами во Второй Мировой войне. Фотография устройства приводится ниже.
Enigma была изобретена в начале 1900-х в Германии Артуром Шербиусом (Arthur Scherbius) и использовалась во второй мировой войне, в частности на подводных лодках для связи с штабом. Enigma имела батарею, позволяющую ей при работе не зависеть от внешних источников энергии, клавиатуру, набор светящихся индикаторов для каждой буквы и набор роторов. Процесс перекоммутации контактов на противоположных сторонах ротора был довольно трудоемким. Фактически приходилось соединять каждую пару отдельно, причем высока была вероятность ошибиться, что привело бы к невозможности расшифровки и отправки шифрограмм, понятных для принимающей

стороны. Поэтому к Enigme, как правило, прилагался набор сменных надлежащим образом скоммутированных роторов. Обычно общее число роторов составляло 5-7 штук. Смена ключа производилась сменой роторов.
Каждый ротор Enigmы содержал 52 контакта (2 х число букв латинского алфавита). Внутреннее устройство ротора схематически показано на рисунке. На рисунке видно, что провода соединяют контакты не по порядку, например 1 верхний контакт соединен с 15-м нижним.



Enigma имела 3 таких ротора работающих вместе (4 в конце войны). Последний ротор соединялся с так называемым рефлектором (или отражающим ротором), назначение которого было – заставить роторы обработать каждую букву дважды (это увеличивало период шифра и соответственно безопасную длину сообщений). Половина из 52 контактов каждого ротора была соединена с клавиатурой и батареей, другая половина – с индикаторами. Каждая кнопка клавиатуры замыкала электрическую цепь и загорался индикатор. Какой именно индикатор загорится зависело от положения роторов и от рефлектора.
Для шифрования или расшифрования немецкий шифровальщик должен был установить роторы в начальное положение – задать ключ. Шифрование выполняялось следующим образом. Шифровальщик вводил с клавиатуры буквы исходного текста и смотрел какая индикатор с какой буквой загорится, после чего следовало изменить положение роторов. Так как роторы вращались после каждой буквы, одна и та же буква могла быть зашифрована по-разному. Буква Z использовалась для пробелов, все числа писались словами. Это повышало надежность передачи и сокращало размер необходимого алфавита.
Несмотря на сложность конструкции и алгоритма, Enigma было взломана в ходе войны. Сначала группа польских криптоаналитиков взломала шифр Enigmы и поделилась принципом вскрытия с англичанами. В ходе войны немцы неоднократно модифицировали Enigmy но англичане продолжали анализ новых версий шифров и успешно вскрывали. Несколько роторных машинок были захвачены на подводных лодках.

Список литературы:

1) Брюс Шнайер “Прикладная криптография”
2) A. Hodges, Alan Turing “The Enigma of Intelligance, Simon and Schuster”
3) B. Kahn “Seizing the Enigma”

Internet:

4) http://www.balakovo.san.ru/~mishin/oreilly/tcpip/puis/ch06_03.htm
5) http://ophil.riva.gomel.by/people/Dennis-M-Richie/crypt.html