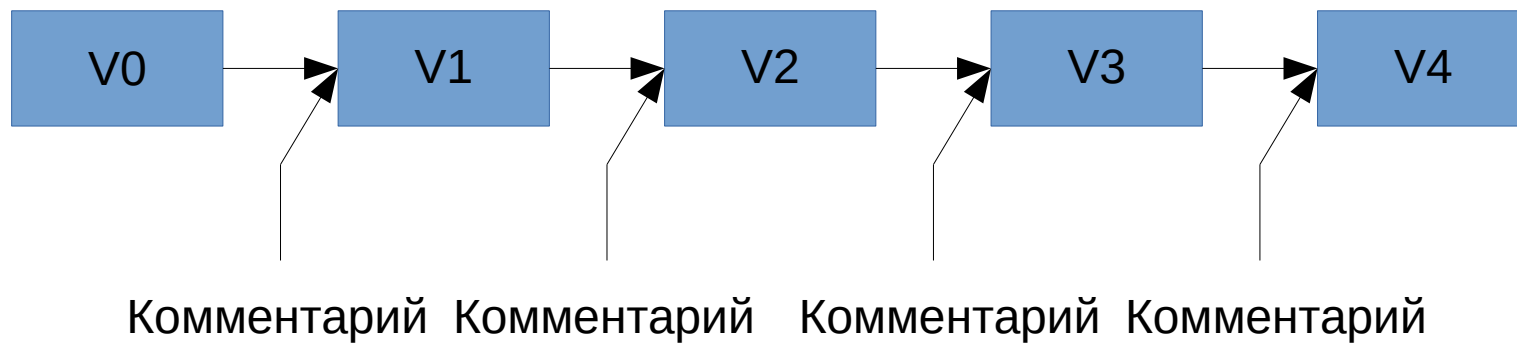


Математические основы информационной безопасности

Груздев Дмитрий Николаевич

Системы контроля версий

Git



Git

Копирование данных с сайта

```
git clone https://github.com/sesc-infosec/sesc-infosec.github.io.git
```

```
git pull origin master
```

Шифры замены

Шифры замены

A, B, C, \dots - алфавит

Функция f – шифр замены, если

$$f(A) \in M_A$$

$$f(B) \in M_B$$

$$f(C) \in M_C$$


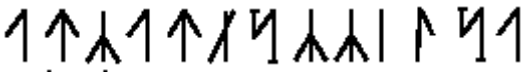
M_A, M_B, M_C, \dots - не пересекаются

$(A-M_A, B-M_B, C-M_C, \dots)$ - ключ шифрования

Шифр простой замены (ШПЗ)

$$|M_A| = 1, |M_B| = 1, |M_C| = 1, \dots$$

Каждая буква алфавита заменяется одним фиксированным символом

- Замена буквы другой буквой
- Шифр “пляшущих человечков” 
- Ж. Верн “К центру земли” 

Шифр масонов

welcome - לרחמים >

Шифр Цезаря

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
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



Юлий Цезарь 100 – 44 гг. до н.э.

welcome - aipgsqi

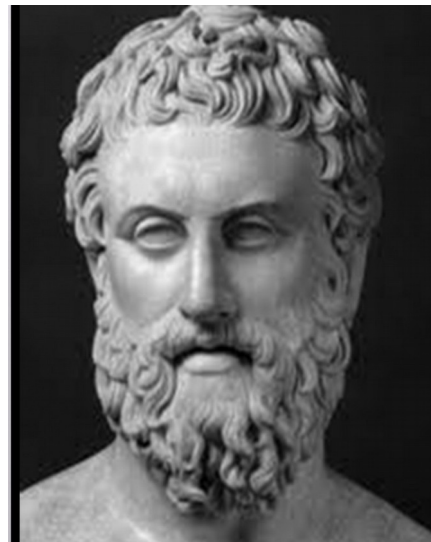
Лозунговый шифр

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

friend - mqdojc

Полибианский квадрат

	1	2	3	4	5	6	7
1	А	Б	В	Г	Д	Е	Ё
2	Ж	З	И	Й	К	Л	М
3	Н	О	П	Р	С	Т	У
4	Ф	Х	Ц	Ч	Ш	Щ	Ъ
5	Ы	Ь	Э	Ю	Я		



Полибий (203-120 гг до н.э.)

МИР – 27'23'34

Система Трисемуса

	1	2	3	4	5	6	7
1	П	Р	И	В	Е	Т	А
2	Б	Г	Д	Ё	Ж	З	Й
3	К	Л	М	Н	О	С	У
4	Ф	Х	Ц	Ч	Ш	Щ	Ъ
5	Ы	Ь	Э	Ю	Я		

Создана в 1508 г.
аббатом Иоганном
Трисемусом

Р – Г

Щ – Т

МИР - ЦДГ

Перестановки

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

A-E-H-D – образуют цикл, записывается как (A,E,H,D) или (E,H,D,A) и т.д.

Вся перестановка: (A,E,H,D)(B,G,O,S,L,W,Z)(C,F,I)(J)
(K,R,P,X,V)(M,Q,N)(T,U)(Y) – циклическая запись

Обратная перестановка

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

Обратная перестановка: сортируем таблицу по нижней строке и меняем строки между собой

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

Обратная перестановка

$$P = (A, E, H, D)(B, G, O, S, L, W, Z)(C, F, I)(J) \\ (K, R, P, X, V)(M, Q, N)(T, U)(Y)$$

Чтобы получить обратную перестановку,
нужно элементы циклов в обратном порядке

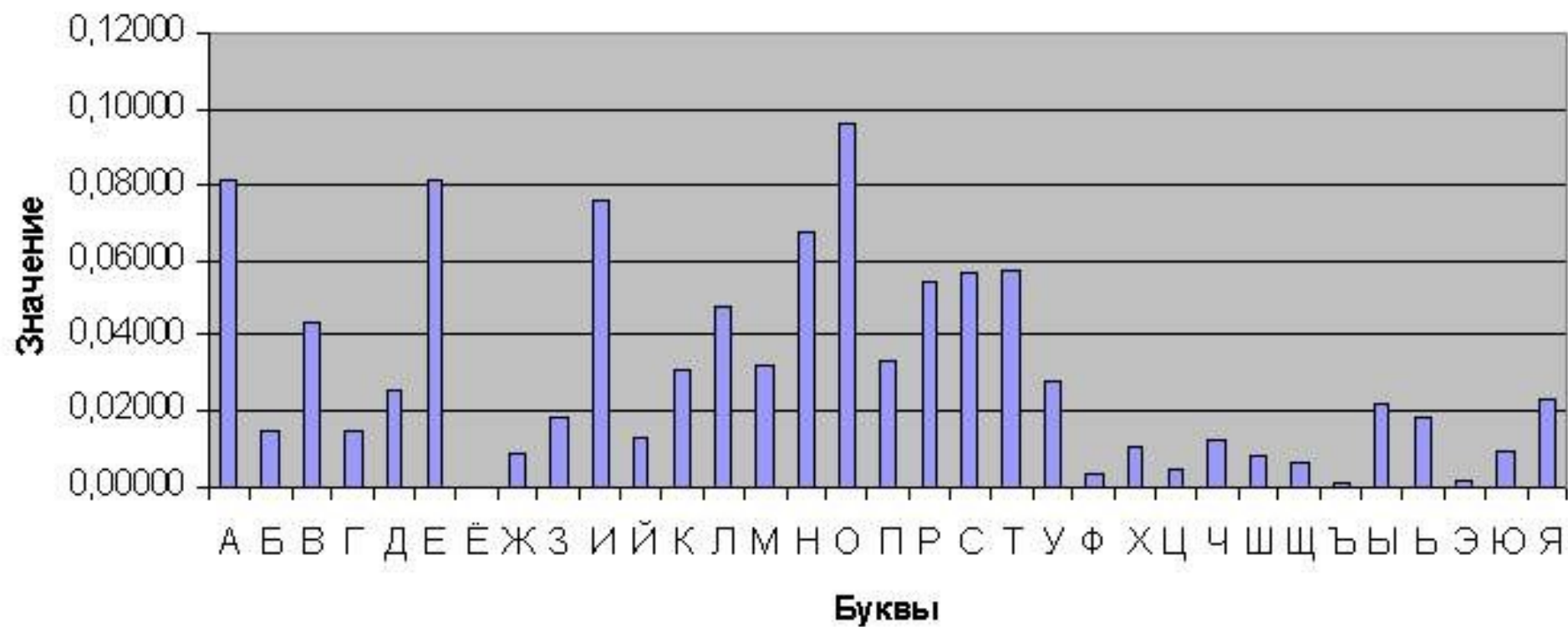
$$P^{-1} = (D, H, E, A)(Z, W, L, S, O, G, B)(I, F, C)(J) \\ (V, X, P, R, K)(N, Q, M)(U, T)(Y)$$

Композиция перестановок

$P_2 \circ P_1$ – перестановка

При последовательном применении нескольких ШПЗ к тексту сложность расшифрования не увеличивается

Частота



Полигамные шифры

Полигамные шифры – это шифры, в которых одна криптозамена соответствует сразу нескольким символам открытого текста.

Создавались для усложнения частотного анализа зашифрованного сообщения.

Шифр Порты

	A	B	C	D		W	X	Y	Z
A	001	002	003	004		023	024	025	026
B	027	028	029	030		049	050	051	052
C	053	054	055	056		075	076	077	078
D	079	080	081	082		101	102	103	104
W	573	574	575	576		595	596	597	598
X	599	600	601	602		621	622	623	624
Y	625	626	627	628		647	648	649	650
Z	651	652	653	654		673	674	675	676

Опубликован в 1563 г.
для алфавита из 20
букв

welcome – welcomez –
we'lc'om'ez –
577'289'377'130 –
577289377130

Шифр Хилла

Предложен в 1929г. математиком Лестером Хиллом.

Текст разбиавается на блоки из n символов.

Ключ шифрования – обратимая матрица A размером $n \times n$.

$$c_i = p_i * A$$

Ключ расшифрования – обратная матрица к A .

$$p_i = c_i * A^{-1}$$

Шифр Хилла

A					A-1			
7	15	4	23		5	22	13	15
6	10	1	0		29	10	20	4
5	2	21	17		10	0	19	2
0	5	12	4		8	4	17	14

МОЛОКОКОРОВЫ – (МОЛО)(КОКО)(РОВЫ) – (13,15,12,15)(11,15,11,15)(17,15,2,28)

$(13,15,12,15) * A = (241,444,499,563) = (10,15,4,2) \bmod 33$

$(11,15,11,15) * A = (222,412,470,500) = (24,16,8,5) \bmod 33$

$(17,15,2,28) * A = (219,549,461,537) = (21,21,32,9) \bmod 33$

$(10,15,4,2)(24,16,8,5)(21,21,32,9) = (\text{ЙОДБ})(\text{ЧПЗЕ})(\text{ФФЯИ}) = \text{ЙОДБЧПЗЕФФЯИ}$

$(10,15,4,2) * A^{-1} = (541\ 378\ 540\ 246) = (13,15,12,15) \bmod 33$

Шифр многозначной замены

Шифр многозначной замены

(омофонический) – шифр подстановки, при котором каждый символ заменяется на один из нескольких символов шифралфавита.

$$|M_A| > 1, |M_B| > 1, |M_C| > 1, \dots$$

Шифр многозначной замены

№	А	Б	В	...	Е	...	О	П	Р	...	Э	Ю	Я
1	012	128	325	...	037	...	064	058	265	...	501	064	106
2	659	556	026	...	700	...	149	073	333	...	248	749	098
...
17	111		061	...	144	...	903	656	476	...			453
...			
38	366		804	123		865	...			
...			
69	095				...		010						
...										
71					541		268						
...							...						
94							479						

“варево” –
325’012’265’037’
026’064

Полиалфавитный шифр

Полиалфавитный шифр – это совокупность шифров простой замены, которые последовательно используются согласно некоторому правилу.

Шифр Виженера

В 1553г. описан в книге Джовани Белассо

Не поддавался вскрытию три века и получил название “неразгадываемого”.

В XIX веке шифр стали называть именем Блеза Виженера – французского дипломата.

Шифр Виженера

	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

ОТ: welcome

П: key

W	E	L	C	O	M	E
K	E	Y	K	E	Y	K
G	I	J	M	S	K	O

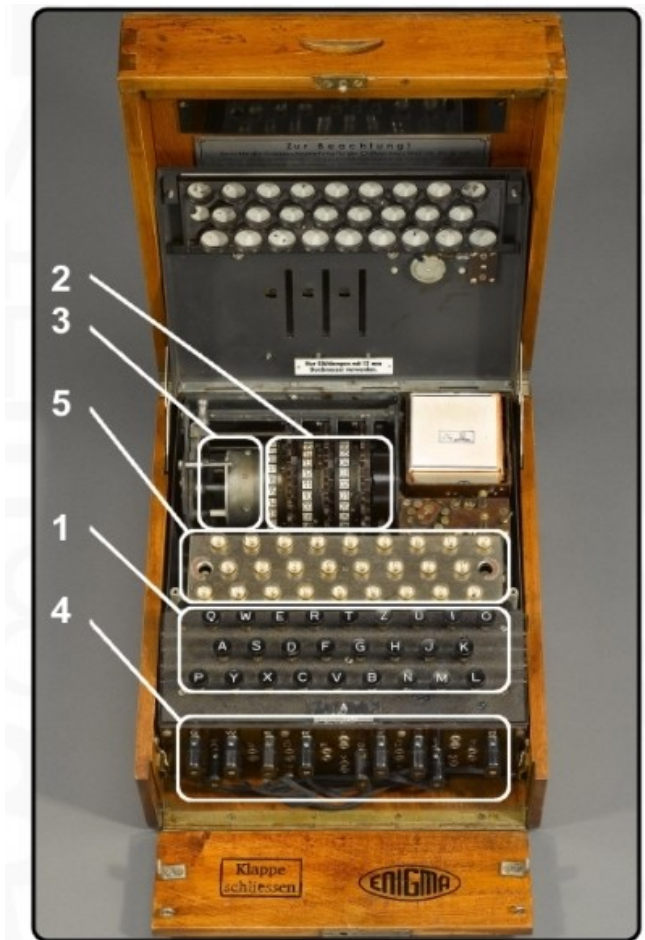
Энигма



1923 г. представлен
первый экземпляр
“Энигмы”.

Использовалась в
Швеции, Польше,
Нидерландах,
Великобритании,
Японии, Италии,
Испании и США.

Энигма



1 – панель механических клавиш

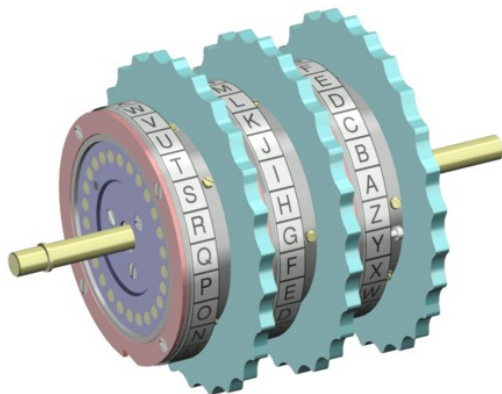
2 – роторные диски

3 – рефлексор

4 – коммутационная панель

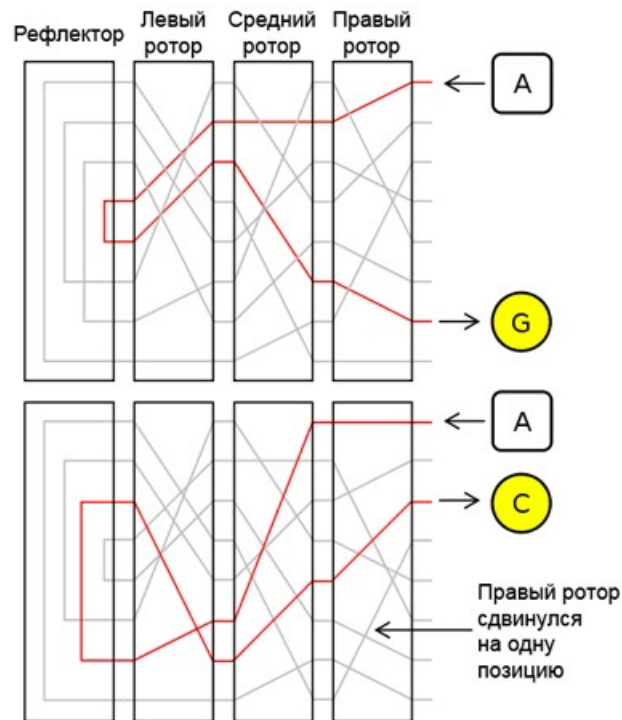
5 – индикационная панель с лампочками

Роторы



Каждый ротор осуществляет шифр простой замены.
Секретом является: выбор роторов, расположение роторов и начальные позиции роторов.

Роторы



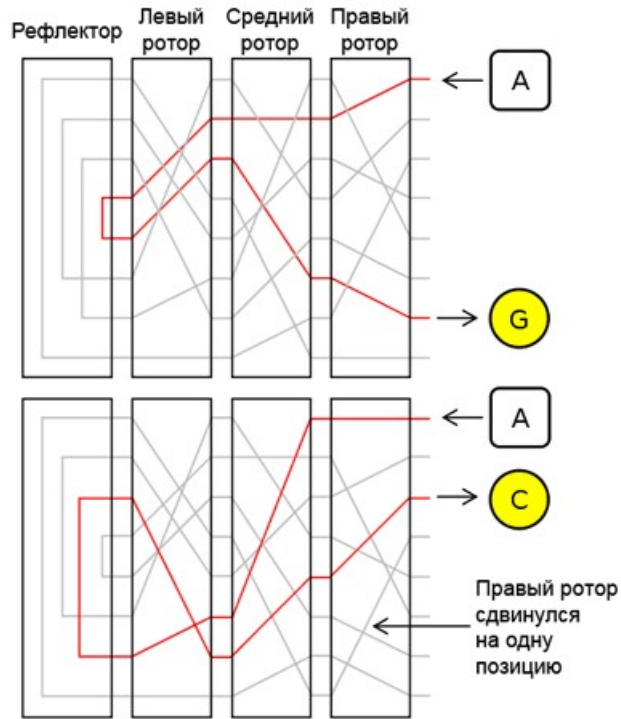
Прохождение электрического сигнала по роторам в процессе шифрования.

После нажатия клавиши роторы поворачиваются.

Варианты роторов

Rotor I	(AELTPHQXRU) (BKNW) (CMOY) (DFG) (IV) (JZ) (S)
Rotor II	(FIXVYOMW) (CDKLHUP) (ESZ) (BJ) (GR) (NT) (A) (Q)
Rotor III	(ABDHPEJT) (CFLVMZOYQIRWUKXSG) (N)
Rotor IV	(AEPLIYWCOXMRFZBSTGJQNH) (DV) (KU)
Rotor V	(AVOLDRWFIUQ)(BZKSMNHYC) (EGTJPX)
Rotor VI	(AJQDVLEOZWIYTS) (CGMNHFUX) (BPRK)
Rotor VII	(ANOUPFRIMBZTLWKSVEGCJYDHXQ)
Rotor VIII	(AFLSETWUNDHOZVICQ) (BKJ) (GXY) (MPR)
Beta Rotor	(ALBEVFCYODJWUGNMQTZSKPR) (HIX)
Gamma Rotor	(AFNIRLBSQWVXGUZDKMTPCOYJHE)
reflector B	(AY) (BR) (CU) (DH) (EQ) (FS) (GL) (IP) (JX) (KN) (MO) (TZ) (VW)
reflector C	(AF) (BV) (CP) (DJ) (EI) (GO) (HY) (KR) (LZ) (MX) (NW) (TQ) (SU)
reflector B Dünn	(AE) (BN) (CK) (DQ) (FU) (GY) (HW) (IJ) (LO) (MP) (RX) (SZ) (TV)
reflector C Dünn	(AR) (BD) (CO) (EJ) (FN) (GT) (HK) (IV) (LM) (PW) (QZ) (SX) (UY)

Шифрование данных



R_L, R_M, R_R – шпз на роторах

C_{LM}, C_{MR} – смещения между алфавитами роторов

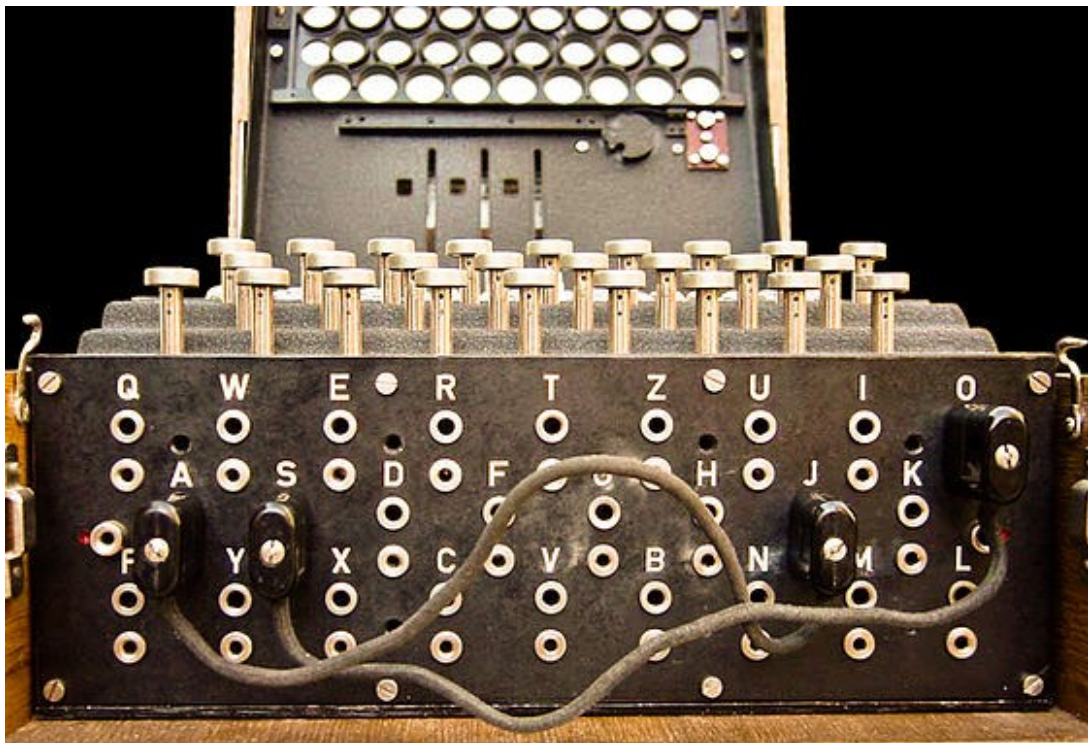
P – шпз на рефлекторе

$$f = R_R C_{MR} R_M C_{LM} R_L P R_L^{-1} C_{LM}^{-1} R_M^{-1} C_{MR}^{-1} R_R$$

C_{LM}, C_{MR} – начальное положение для каждой сессии

R_L, R_M, R_R, P – для комплекта устройств

Коммутационная панель



Перед шифрованием на роторах и после шифрования на них заменяла пары выбранных букв между собой.

На рисунке выбраны две пары: S-J и A-O.

Пары могут быть выбраны перед каждым сеансом.

Энигма

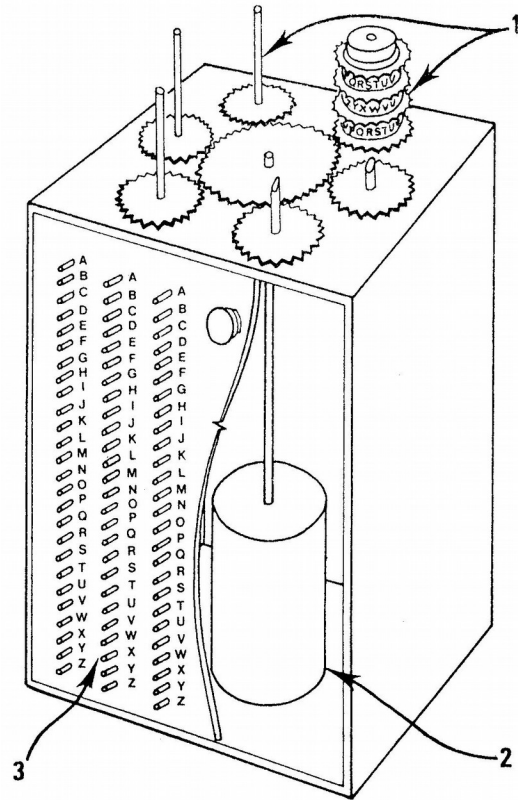
$$f = KR_R C_{MR} R_M C_{LM} R_L P R_L^{-1} C_{LM}^{-1} R_M^{-1} C_{MR}^{-1} R_R^{-1} K^{-1}$$

1938 г. польский криптоаналитик Мариан Реевски создал “криптологическую бомбу” для расшифровки немецких сообщений.

1939 г. немецкие криптографы увеличили сложность шифрования материалов на Энигме.

1940 г. в Англии была запущена “Turing bombe” - более эффективное устройство, восстанавливающее текст, если была известна его структура или часть открытого текста.

Энигма



Bomba kryptologiczna

