

# *Формальная криптография*

*(конец XV века - начало XX века)*

# Аддитивный шифр

- Заменим буквы алфавита числами, соответствующими их порядковым номерам в алфавите  $0, 1, \dots, n-1$

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$n = 26$

- Представим символы открытого текста  $P_i$  и шифротекста  $C_i$  соответствующими числами
- Выбираем в качестве ключа число  $k$
- Шифрование символа:  $C_i = (P_i + k) \bmod n$
- Расшифровка символа:  $P_i = (C_i - k) \bmod n$
- Случай  $k = 3$  - шифр Цезаря

# Пример атаки на аддитивный шифр

- Шифр уязвим к атакам методом «грубой силы»
- Множество ключей аддитивного шифра равно числу букв алфавита
- Нулевой ключ, является бесполезным (зашифрованный текст будет совпадать с исходным текстом). Требуется перебор  $n-1$  возможных ключей

# Мультипликативный шифр

- Заменим буквы алфавита числами, соответствующими их порядковым номерам в алфавите  $0, 1, \dots, n-1$

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$n = 26$

- Представим символы открытого текста  $P_i$  и шифротекста  $C_i$  соответствующими числами
- Выбираем в качестве ключа число  $k, 1 \leq k < n$ ,  
 $k \times k^{-1} \equiv 1 \pmod n$  (существует мультипликативная инверсия)
- Шифрование символа:  $C_i = (P_i \times k) \pmod n$
- Расшифровка символа:  $P_i = (C_i \times k^{-1}) \pmod n$

# Пример атаки на мультипликативный шифр

- Шифр уязвим к атаке методом «грубой силы»
- Множество ключей мультипликативного шифра равно числу ключей аддитивного шифра, имеющих мультипликативную инверсию, например для  $n=26$ :

$k =$	1	3	5	7	9	11	15	17	19	21	23	25
$k^{-1} =$	1	9	21	15	3	19	7	23	11	5	17	25

- Требуется перебор в худшем случае  $n-1$  возможных ключей

# Аффинный шифр

- Является комбинацией аддитивного и мультипликативного шифров
- Ключ состоит из двух частей  $k_1$  и  $k_2$
- Шифрование символа:  $C_i = (P_i \times k_1 + k_2) \bmod n$
- Расшифровка символа:  $P_i = ((C_i - k_2) \times k_1^{-1}) \bmod n$
- При  $k_1 = 1$  - аддитивный шифр
- При  $k_1 = -1$  и  $k_2 = 25$  - шифр Атбаш
- При  $k_2 = 0$  - мультипликативный шифр

# Примеры атак на аффинный шифр

- Сложность атаки «грубой силы»  $\varphi(n) \times n$ ,  $\varphi(n)$ - функция Эйлера
  - Атака на основе открытого или выбранного текста:
    - Предполагаем, что известны биграмма  $P_i P_{i+1}$  и ее шифр  $C_i C_{i+1}$
    - Решаем систему уравнений:
$$\begin{cases} C_i = (P_i \times k_1 + k_2) \bmod n \\ C_{i+1} = (P_{i+1} \times k_1 + k_2) \bmod n \end{cases}$$
- Определяем  $k_1 = \left( (C_{i+1} - C_i) \times (P_{i+1} - P_i)^{-1} \right) \bmod n$ , затем  $k_2$
- В случае нескольких решений, ориентируемся на связность расшифрованного текста

# Шифр моноалфавитной подстановки (substitution)

➤ Открытый текст:

HELLO

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

➤ Шифротекст:

PASSWORD >> 3

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

OAGGJ



# Пример атаки

- Сложность атаки «грубой силы» при  $n = 26$  составляет  $26!$ , (примерно  $4 \times 10^{26}$ )
- Возможна атака методом частотного анализа:
  - Подсчитывается частота появления каждой буквы шифротекста
  - Полученное распределение частот сравнивается, например, со справочной таблицей частот для символов языка открытого текста
  - Выдвигаются гипотезы о соответствии букв открытого текста и шифротекста
  - Сделанные гипотезы проверяются с помощью справочных таблиц распределения биграмм и триграмм

# Частотные характеристики букв русского языка

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
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

## • Наиболее вероятные биграммы

"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".

## • Наиболее вероятные триграммы

"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".

# Частотные характеристики 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

## Наиболее вероятные биграммы

"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".

## Наиболее вероятные триграммы

"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".

# Омофонический шифр (1401)

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
8.2	1.2	4.1	4.1	11.8	1.9	1.1	3.0	8.3	0.1	0.3	4.4	2.1	9.2	8.3	2.9	0.1	6.1	5.1	8.8	2.8	1.6	0.7	0.1	1.0	0.1
8	1	4	4	11	2	2	3	8	1	1	4	3	9	8	3	1	6	5	8	2	2	1	1	1	1
86, 3, 60, 14, 67, 42, 84, 41	36	95, 92, 38, 2	81, 48, 15, 80	98, 76, 40, 79, 75, 69, 62, 61, 82, 51, 5	68, 29	96, 21	47, 74, 99	46, 52, 19, 33, 93, 94, 89, 9	63	83	45, 57, 16, 13	0, 65, 72	24, 7, 34, 12, 26, 1, 32, 30, 73	44, 87, 77, 97, 18, 90, 10, 23	20, 22, 37	35	17, 39, 91, 11, 50, 25	64, 85, 27, 55, 58	71, 70, 28, 53, 43, 31, 66, 54	6, 49	78, 8	56	59	88	4



Алфавит открытого текста



Частота встречаемости букв



Кол-во омофонов (для 100 символов шифрующего алфавита)



Набор омофонов

# Демонстрация омофонического шифра в CrypTool 1

Key Entry: Homophonic Substitution

Total count and bit length of the homophones  
Total    
Bit  bits

Encryption options  
Consider input document as ☐ Include formatting with encryption  
☒ Text ☐ Binary data


Key table for homophonic substitution

Ord	Char...	Frequ...	Count	List of homophones
71	G	1.1	2	96, 21
72	H	3.0	3	47, 74, 99
73	I	8.3	8	46, 52, 19, 33, 93, 94, 89, 9
74	J	0.1	1	63
75	K	0.3	1	83
76	L	4.4	4	45, 57, 16, 13
77	M	2.1	3	0, 65, 72
78	N	9.2	9	24, 7, 34, 12, 26, 1, 32, 30,
79	O	8.3	8	44, 87, 77, 97, 18, 90, 10, 2
80	P	2.9	3	20, 22, 37
81	Q	0.1	1	35
82	R	6.1	6	17, 39, 91, 11, 50, 25
83	S	5.1	5	64, 85, 27, 55, 58
84	T	8.8	8	71, 70, 28, 53, 43, 31, 66, 5
85	U	2.8	2	6, 49
86	V	1.6	2	78, 8
87	W	0.7	1	56
88	X	0.1	1	59
89	Y	1.0	1	88
90	Z	0.1	1	4

Display of homophones  
☐ Hexadecimal ☒ Decimal

Show the list of homophones for individual characters:

Characters	Number	List of homophones
Z	1	4



# Шифр Виженера (XVI)

➤ **Открытый текст:**

# ПРИМЕРШИФРАВИЖЕНЕРА

Diagram illustrating the mapping of a 2x4 grid of Cyrillic letters to a 5x30 Cyrillic alphabet grid. The 2x4 grid has rows: П Р И М, К Л Ю Ч. The 5x30 grid has rows: А-Я, К-Ш, Л-Щ, Ю-Ъ, Ч-Ь. Arrows show the mapping: П to П (row 1, col 16), К to К (row 2, col 1), Л to Л (row 2, col 2), Ю to Ю (row 3, col 1), and Ч to Ч (row 4, col 1).

 Шифротекст:

ШЪЖВПЪЦЯЭЪЮЩТСГГПЪЮ

# Формальная модель шифра Виженера

- Заменим буквы алфавита числами, соответствующими их порядковым номерам в алфавите  $0, 1, \dots, n$

А	Б	В	Г	Д	Е	Ж	З	И	К	Й	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

- Представим символы открытого текста  $P_i$ , ключа  $K_i$  и шифротекста  $C_i$  соответствующими числами
- Сформируем гамму повторением ключа

$$G = (K_1, \dots, K_m) \dots (K_1, \dots, K_m)$$

- Шифрование символа:  $C_i = (P_i + G_i) \bmod n$
- Расшифровка символа:  $P_i = (C_i - G_i) \bmod n$

# Криптоанализ шифра Виженера

- Сложность атаки грубой силы  $\frac{n!}{(n-m)!}$
- Шифр рассматриваться, как комбинации аддитивных шифров
- Первый этап анализа – определение длины ключевого слова
- Вторым этапом анализа – разделение шифротекста на части, зашифрованных одинаковым символом ключа и анализ полученных частей методами статистического анализа для поиска всех символов ключа



# Этап 1: Автокорреляционный метод

- Метод позволяет отыскать длину ключевого слова в многоалфавитном шифре
- Шифротекст, длиной  $L$ , выписывается в строку, а под ней выписываются строки, полученные сдвигом влево на  $t = 1, 2, 3, \dots$  позиций. Для каждого  $t$  подсчитывается число  $n_t$  совпадений символов находящихся на одинаковых позициях в шифротексте и его версии со сдвигом  $t$
- Вычисляются автокорреляционные коэффициенты  $K_t = \frac{n_t}{L-t}$
- Для сдвигов, кратных периоду ключа, коэффициенты  $K_t$  будут заметно больше, чем для сдвигов, не кратных периоду и иметь значение близкое к индексу совпадений используемого языка (для русского языка  $\sim 0.0553$ )
- Соответствующие сдвиги  $t$  берутся в качестве оценки длины ключа

# Пример использования автокорреляционного метода

## ➤ Шифротекст:

ШЪЖВПЪЦЯЭЪЮЩТСГГПЪЮ

ЪЖВПЪЦЯЭЪЮЩТСГГПЪЮШ

ЖВПЪЦЯЭЪЮЩТСГГПЪЮШЪ

ВПЪЦЯЭЪЮЩТСГГПЪЮШЪЖ

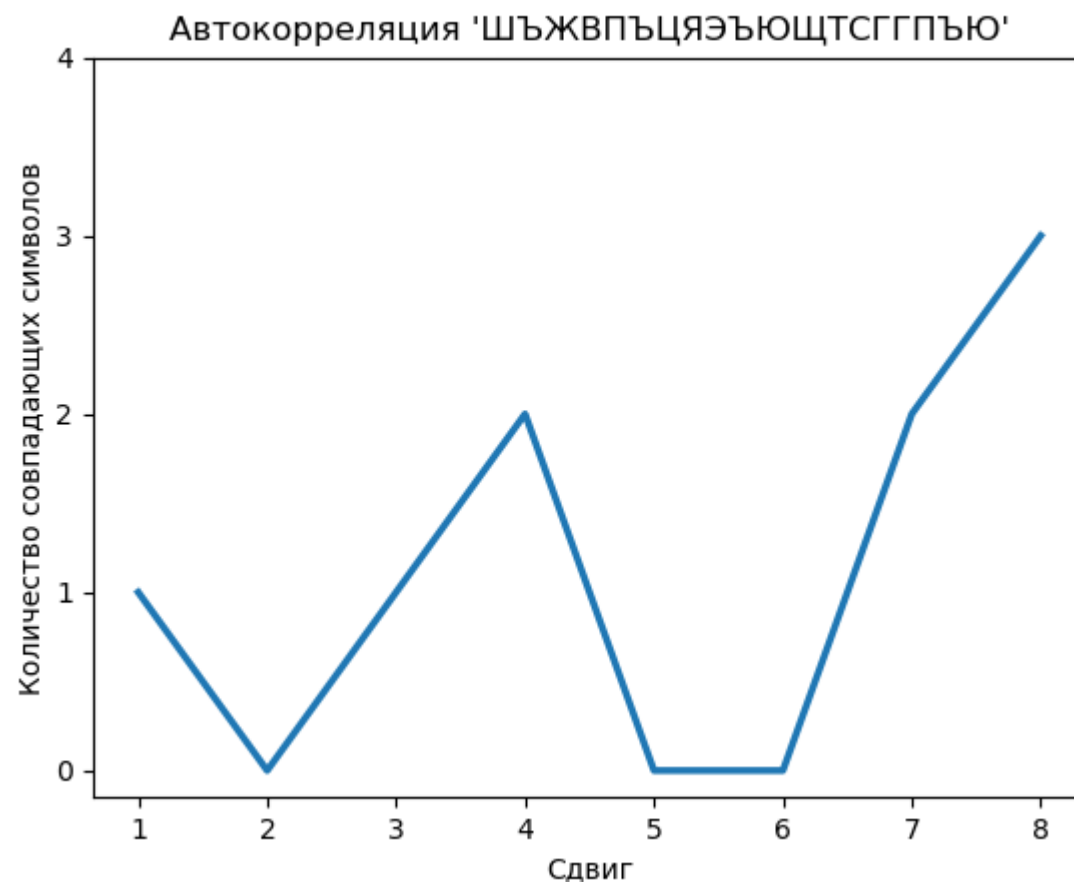
ПЪЦЯЭЪЮЩТСГГПЪЮШЪЖВ

ЪЦЯЭЪЮЩТСГГПЪЮШЪЖВП

ЦЯЭЪЮЩТСГГПЪЮШЪЖВПЪ

ЯЭЪЮЩТСГГПЪЮШЪЖВПЪЦ

ЭЪЮЩТСГГПЪЮШЪЖВПЪЦЯ



# Этап 2: Статистический метод

Ш Ъ Ж В

П Ъ Ц Я

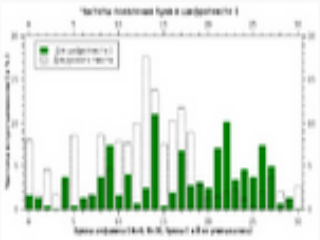
Э Ъ Ю Щ

Т С Г Г

П Ъ Ю

- Анализируются фрагменты шифротекста, зашифрованные одной и той же буквой шифра

- По возможности (в случае больших текстов) применяются методы частотного анализа



# Свойства рассмотренных шифров

- Симметричность – отправитель и получатель обладают одинаковыми секретными ключами и одинаковыми алгоритмами для зашифрования и расшифрования
- Поточность - каждый символ открытого текста преобразуется в символ зашифрованного текста в зависимости не только от используемого ключа, но и от расположения символа в потоке открытого текста
- Основаны преимущественно на операциях перестановки и замены (подстановки)

# Шифр двойной перестановки

➤ Открытый текст:

ПРИМЕРМАРШРУТНЫЙШИФР



➤ Шифротекст:

ФРИШЙМЕИРПНЫТУРРШАМР

# Пример атаки

- Сложность атаки «грубой силы»  $n! \times m!$ , где  $n$  и  $m$  – количество строк и столбцов соответственно
- Для расшифровки применим частотный анализ биграмм
- Предпринимаются попытки определить размер столбца, поскольку известно, что длина шифротекста кратна этому размеру
- Отсев гипотез при перестановках основывается на обнаружении запретных биграмм
- Выбранный вариант перестановки может оказаться ложным (существуют анаграммы, например КЛОУН-КОЛУН-КУЛОН-УКЛОН)
- Желательно знание фрагментов открытого текста

# Шифр Плейфера (1914)

➤ Открытый текст:

HELLO



HE LL O



HE LX LO



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



Матрица-ключ

➤ Шифротекст:



EC QZ BX

# Пример атаки

- Сложность атаки «грубой силы» 25!
- Шифр скрывает частоту отдельных букв
- Возможна атака, основанная на анализе частоты биграмм, чтобы найти ключ
- Атака существенно упрощается, если известен фрагмент исходного текста, например, стандартная форма обращение к адресату (Dear Sirs)



# Шифр Хилла : зашифрование (1929)

➤ Открытый текст:

HILLCIPHEREXAMPLES

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	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

7	8	11
11	2	8
15	7	4
17	4	23
0	12	15
11	4	18



6	24	1
13	16	10
20	17	15

Шифрующая  
матрица



366	483	252
252	432	151
261	540	145
614	863	402
456	447	345
478	634	321



2	15	18
18	16	21
1	20	15
16	5	12
14	5	7
10	10	9

(mod 26)

➤ Шифротекст:

CPSSQVBUPQFMOFHKKJ

# Шифр Хилла: расшифрование<sup>(1929)</sup>

➤ Шифротекст:

CPSSQVBUPQFMOFHKKJ

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	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

2	15	18
18	16	21
1	20	15
16	5	12
14	5	7
10	10	9



8	5	10
21	8	21
21	12	8

Дешифрующая  
матрица  
(обратная)



709	346	479
921	470	684
743	345	550
485	264	361
364	194	301
479	238	382



7	8	11
11	2	8
15	7	4
17	4	23
0	12	15
11	4	18

(mod 26)

➤ Открытый текст:

HILLCIPHEREXAMPLES

# Шифр Хилла: свойства шифрующей матрицы

- В общем случае матрица шифрования квадратная  $t \times t$ , где  $t$  – размер блока текста, подлежащего зашифрованию
- Матрица обратима в том и только в том случае, когда ее детерминант не равен нулю и не имеет общих делителей с основанием модуля
- Обратная матрица  $M^{-1}$  является мультипликативной инверсией  $M$  в  $\mathbf{Z}_{26}$  (см. «Модульная арифметика»)  
$$M \times M^{-1} \equiv I \mod 26$$

# Пример атаки

- Сложность атаки методом «грубой силы» в худшем случае  $n^{m \times m}$
- Шифр не сохраняет статистику обычного текста
- Возможна атака на ключ на основе знания исходного текста:
  - Делается предположение о размере блока (например,  $m$ )
  - Добываются не менее  $m$  пар блоков открытого текста и шифротекста и строится уравнение  $C = P \times K$
  - Выполняется попытка восстановить матрицу-ключ  $K = C \times P^{-1}$
  - В случае неудачи выбирается другой размер блока  $m$

# Комбинированный шифр ADFGVX (1918)

## ❖ Шаг 1: Замена

➤ Открытый текст: CIPHEREXAMPLE

	A	D	F	G	V	X
A	A	B	C	D	E	F
D	G	H	I	J	K	L
F	M	N	O	P	Q	R
G	S	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

AF DF FG DD AV FX AV GX AA FA FG DX AV

# Комбинированный шифр ADFGVX<sup>(1918)</sup>

## ❖ Шаг 2: Перестановка

➤ Текущий текст: AF DF FG DD AV FX AV GX AA FA FG DX AV

О	U	R	K	E	Y
3	5	4	2	1	6
A	F	D	F	F	G
D	D	A	V	F	X
A	V	G	X	A	A
F	A	F	G	D	X
A	V				

Е	К	О	Р	У	Y
1	2	3	4	5	6
F	F	A	D	F	G
F	V	D	A	D	X
A	X	A	G	V	A
D	G	F	F	A	X
		A		V	

➤ Шифротекст:

FFADF VXGAD AFADA GFFDV AVGXA X

# Почему шифр назван ADFGVX ?

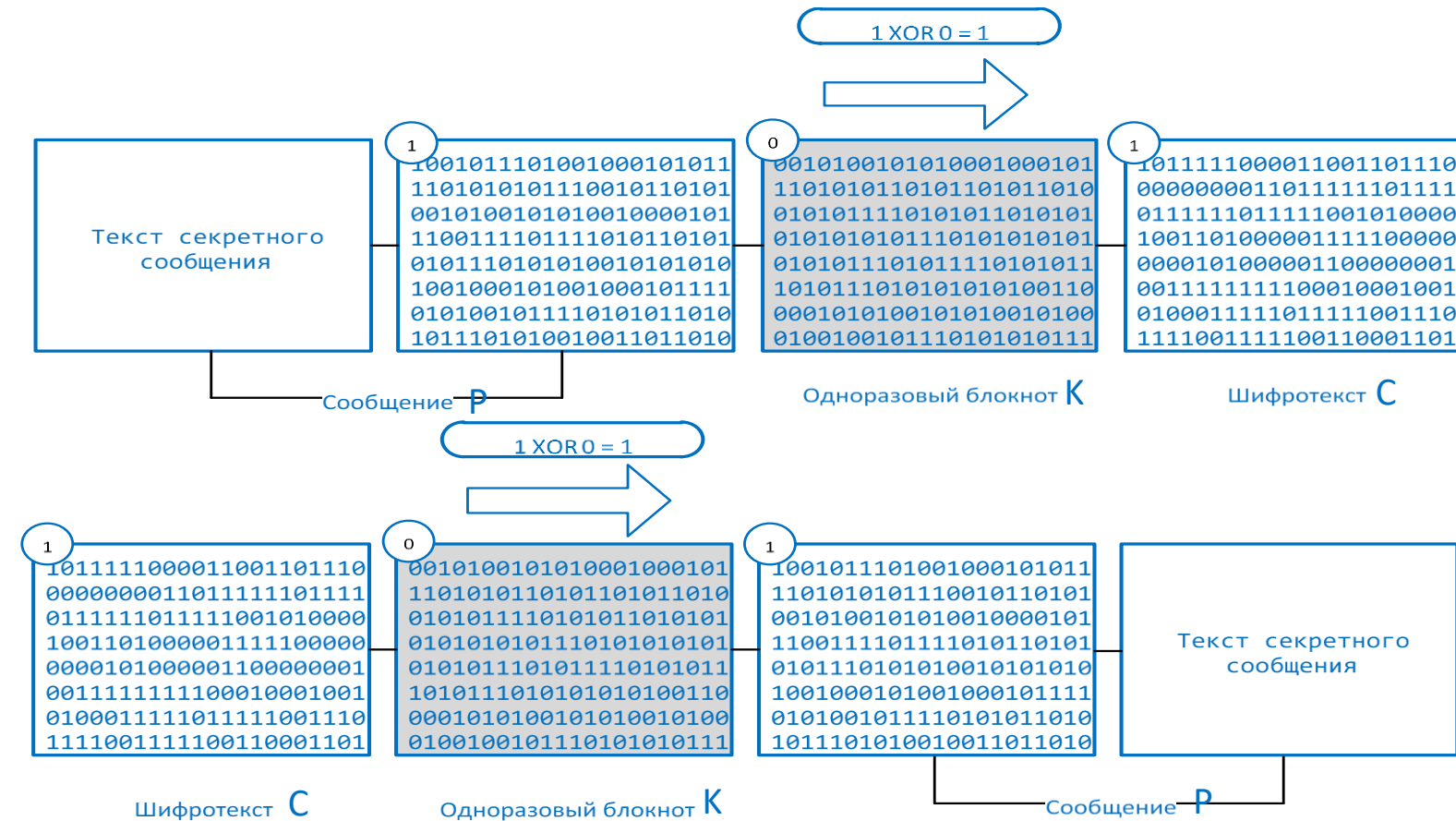
Буква	Код
A	
D	
F	
G	
V	
X	

# Пример атаки

- Атаки основаны знании фрагментов открытого текста:
  - На основе анализа 2-х и более сообщений с одинаковым начальным текстом
  - На основе анализа 2-х и более сообщений с одинаковым окончанием
  - На основе сообщений одинакового размера
- Определяется перестановка, а затем частотным анализом шифрующая матрица



# Шифр Вернама (1917)



Одноразовый шифровальный блокнот -one-time pad (OTP):  $C = P \oplus K$ ;  $P = C \oplus K$

# Одноразовая зашифровка и расшифровка

➤ Открытый текст:

➤ Ключ:

➤ Шифротекст:

Р	1	1	0	1	0	0	1	1	1	0	0
К	1	0	0	1	1	0	0	1	1	0	0
С	0	1	0	0	1	0	1	0	0	0	0

Зашифровка  $C = P \oplus K$

Расшифровка  $P = C \oplus K$

х	у	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

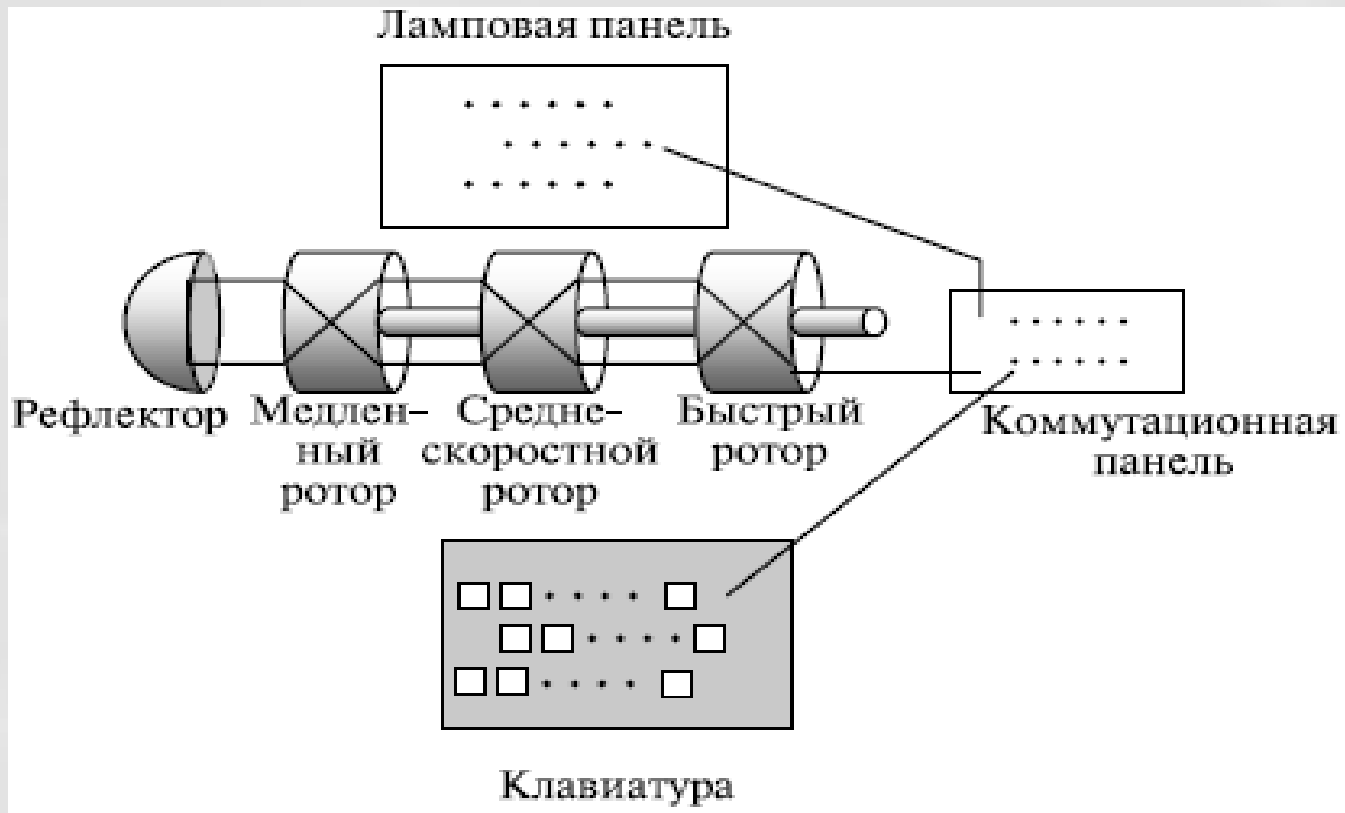
# Требования к одноразовому блокноту

- Должен состоять из действительно случайных значений
- Должен использоваться только один раз
- Должен безопасно передаваться получателю
- Должен быть надежно защищен, как на стороне отправителя, так и на стороне получателя

# Атака на двухразовый блокнот

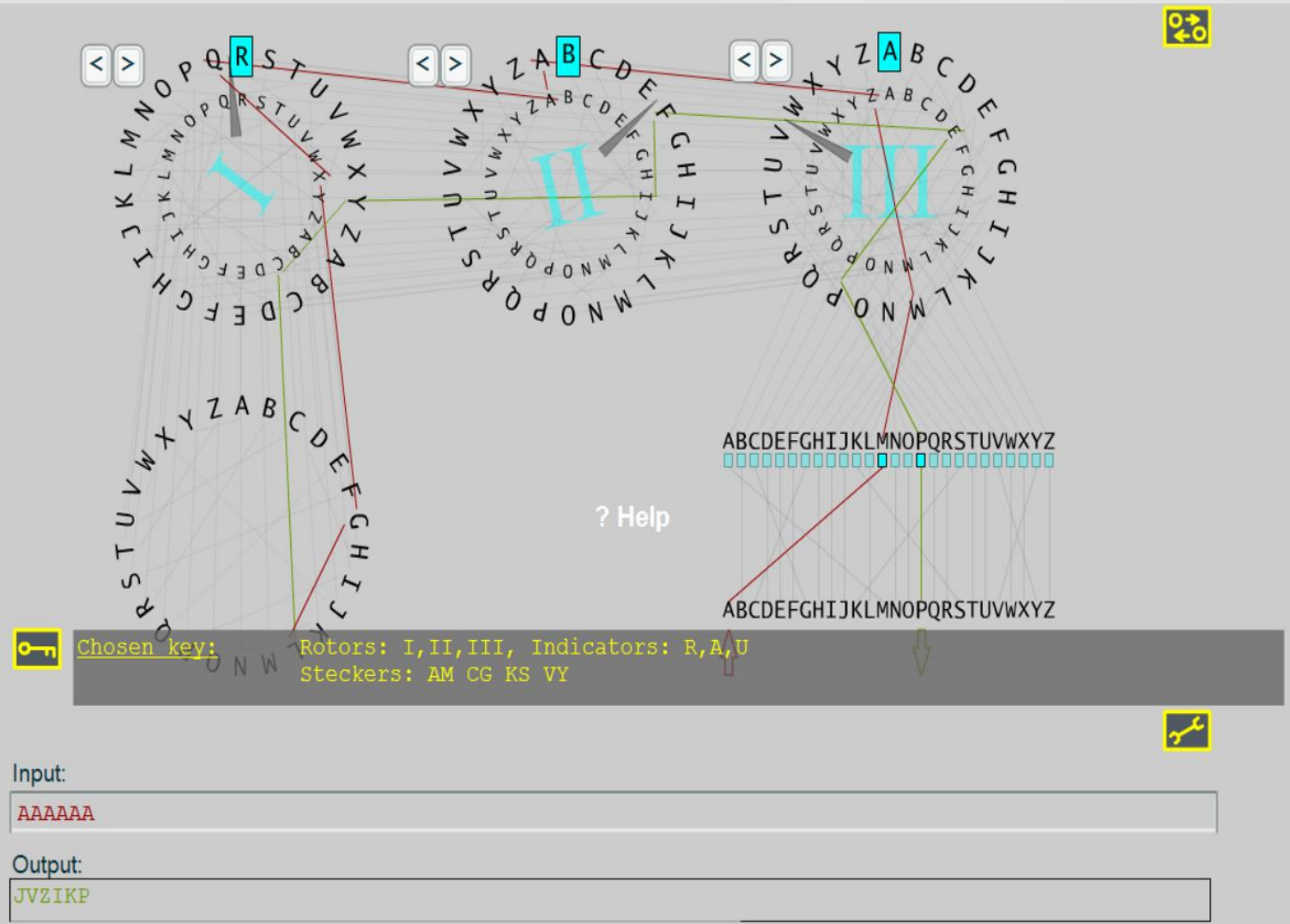
- $C_1 = P_1 \oplus K; C_2 = P_2 \oplus K$
- $K = C_1 \oplus P_1; K = C_2 \oplus P_2$
- $C_1 \oplus P_1 = C_2 \oplus P_2$
- **$P_1 = C_1 \oplus C_2 \oplus P_2$**

# Шифровальная машина (1923)



- Клавиатура для ввода исходного текста или шифровки
- Коммутационная панель (штекеры) для начальной подстановки символов
- Ламповая панель для индикации результатов
- Роторы (диски) с 26 контактами и внутренней прошивкой для реализации подстановки
- Рефлектор для обеспечения единообразия процесса зашифрования и расшифрования

# Модель машины «Энигма»

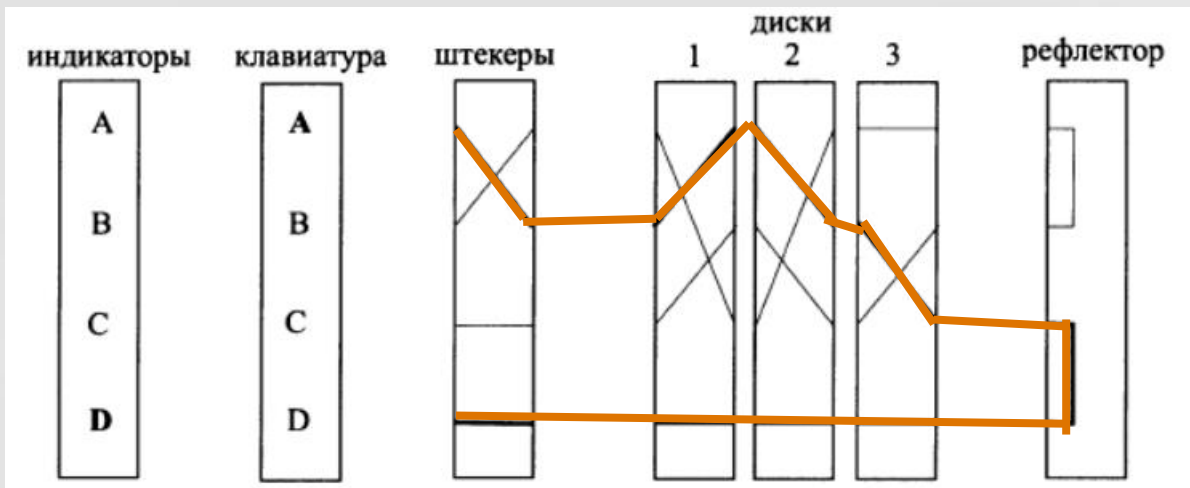


## Ключ:

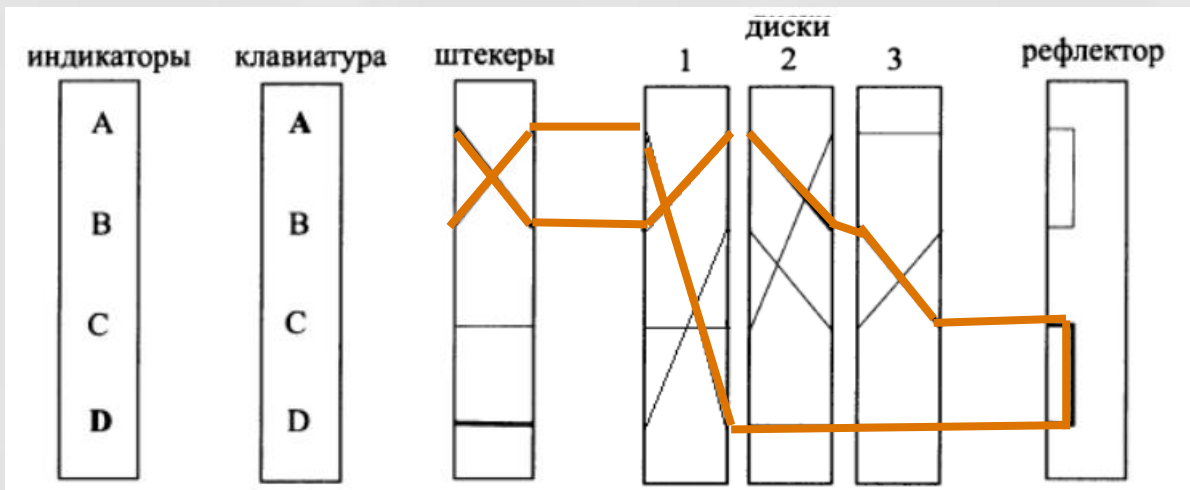
- ❖ Порядок следования роторов
- ❖ Исходные положение каждого ротора
- ❖ Настройка коммуникационной панели



# Зашифровка и расшифровка



- Исходный текст: **A**
  - Подстановки: A-B-A-B-C-D-D-D-D-D
- Шифротекст: **D**
  - Поворот диска 1



- Исходный текст: **AA**
  - Подстановки: A-B-A-B-C-D-D-D-A-B
- Шифротекст: **DB**
  - Поворот диска 1

# Пример атаки на машину «Энигма»

- Сложность атаки «грубой силы» для количества пар коммутаций  $m = 10$  составляет  $\approx 2^{64}$  вариантов
- Возможна атака с известным открытым текстом:
  - <https://habrahabr.ru/post/269519/>
  - В паре открытый текст-шифротекст находятся циклы

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
w	e	t	t	e	r	v	o	r	h	e	r	s	a	g	e	b	i	s	k	a	y	a
r	w	i	v	t	y	r	e	s	x	b	f	o	g	k	u	n	q	b	a	i	s	e

- При наличии циклов, задачу взлома можно разделить на простые составные части:
  - поиск стартового положения роторов  $3! \times 26^3 \approx 2^{17}$
  - поиск соединений коммутационной панели при известных установках роторов (моноалфавитная подстановка)  $\approx 2^{47}$



# Принципы Керкгоффса (1883)

- система должна быть не раскрываемой, если не теоретически, то хотя бы практически
- система должна быть простой. Она не должна требовать ни запоминания длинного перечня правил, ни большого умственного напряжения
- **компрометация системы не должна причинять неудобства ее пользователям**
- секретный ключ должен быть легко запоминаемым без каких либо записей
- криптограмма должна быть представлена в такой форме, чтобы ее можно было передать по телеграфу
- аппаратура шифрования должна быть портативной и такой, чтобы ее мог обслуживать один человек

