Crypto

Криптография

- **Криптогра́фия** (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), шифрования.

История криптографии

Периоды развития криптографии:

- Первый период - примерно с 3 тысячелетия до н.э. – моноалфавитные шифры;
- Второй период - с IX века на Ближнем Востоке и с XV века в Европе – полиалфавитные шифры;
- Третий период - с начала и до середины XX века – внедрение электромеханических устройств;
- Четвертый период - с середины до 70х годов XX века – математическая криптография;
- Современный период – с 70х годов XX века по настоящее время – криптография с открытым ключом.

Криптография в Древнем Мире

Первое известное применение криптографии зафиксировано 4000 лет назад в Древнем Египте

Атбаш

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

Исходный текст	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Зашифрованный текст	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б	А

Скитала

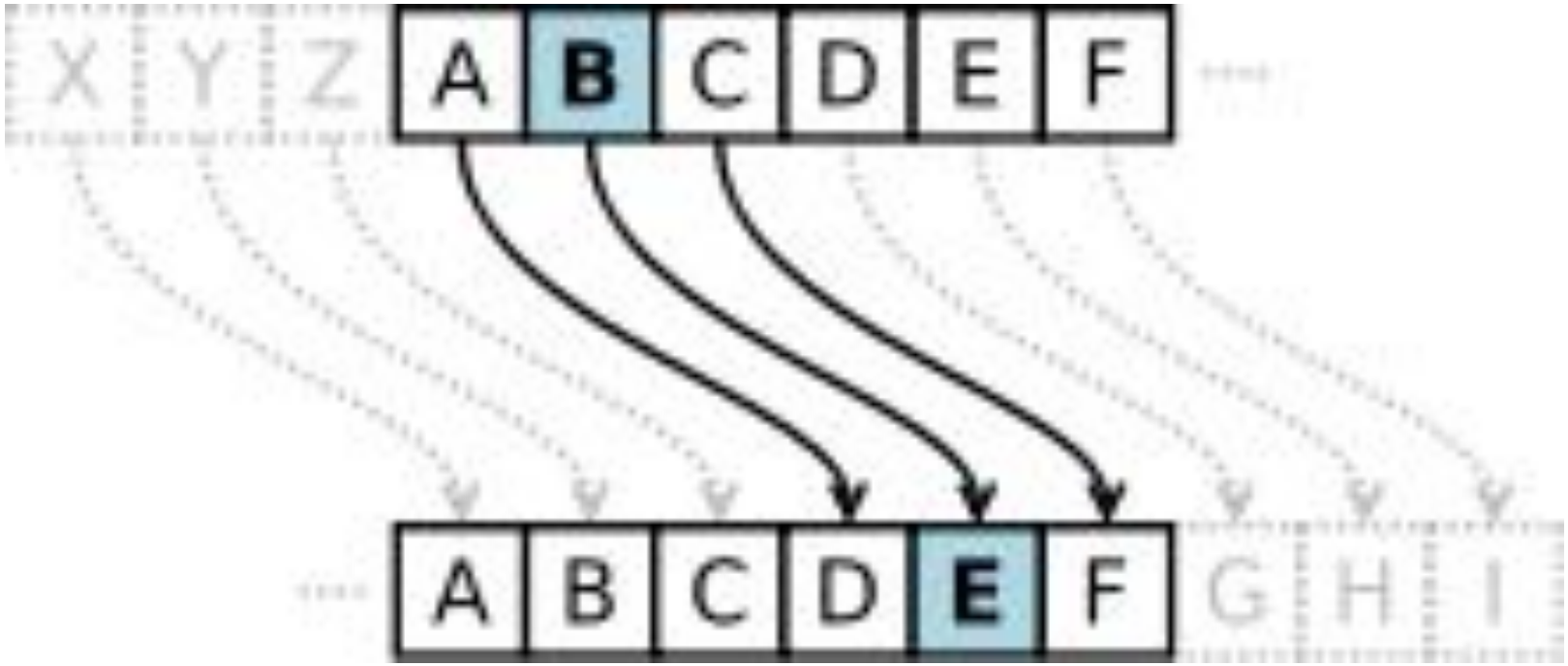
- Скитала или сцитала представляла собой длинный стержень, на который наматывалась лента из пергамента. На ленту наносился текст вдоль оси скиталы, так, что после разматывания текст становился нечитаемым. Для его восстановления требовалась скитала такого же диаметра.

Квадрат Полибия

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

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

Шифр Цезаря



Криптография в арабских странах

С VIII века н. э. развитие криптографии происходит в основном в арабских странах.

Первое упоминание о частотном криптоанализе

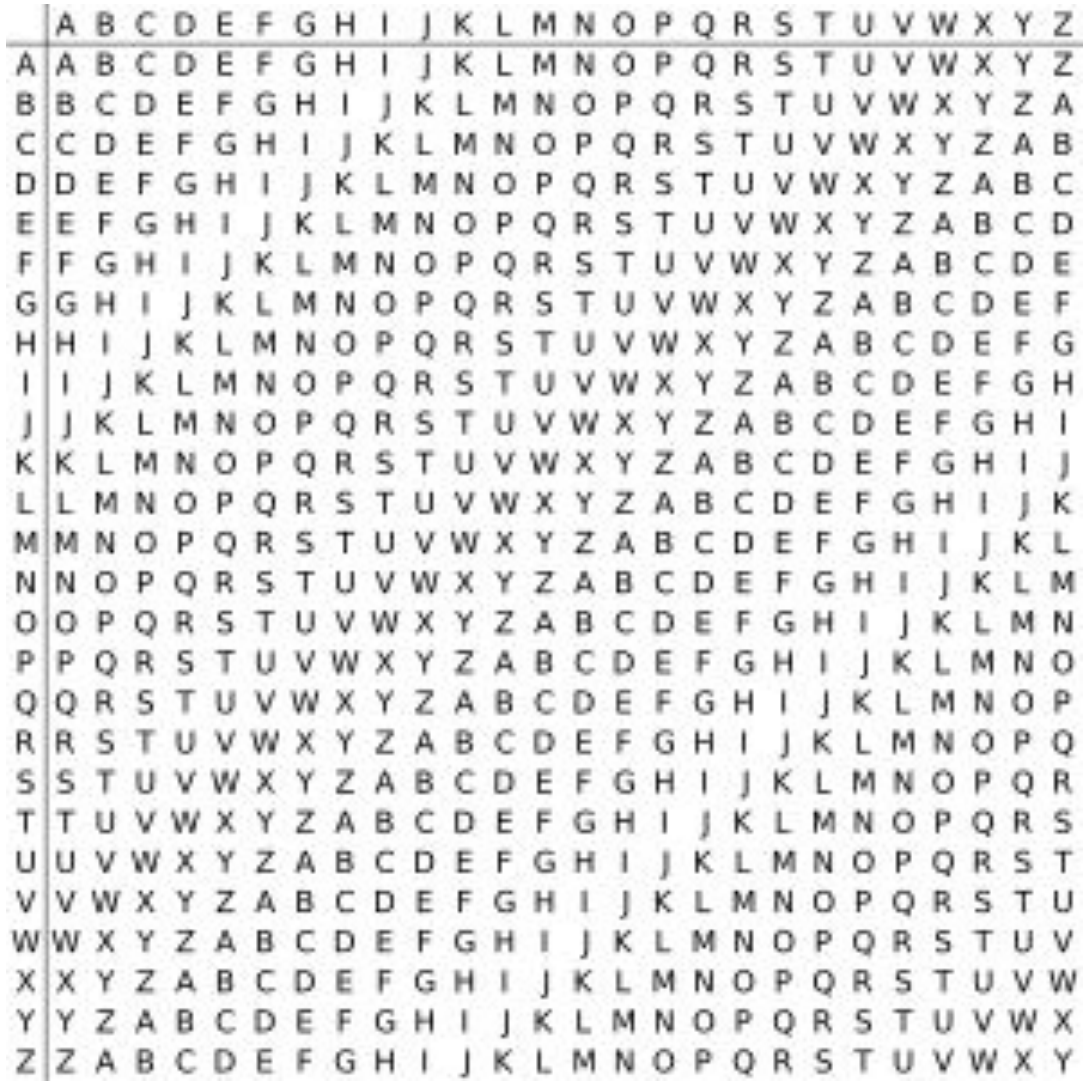
Криптография Эпохи Возрождения

Отец современной криптографии – Леон Баттиста Альберти

Криптография Эпохи Возрождения

Головная боль математиков своего времени - Блез де Виженер

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

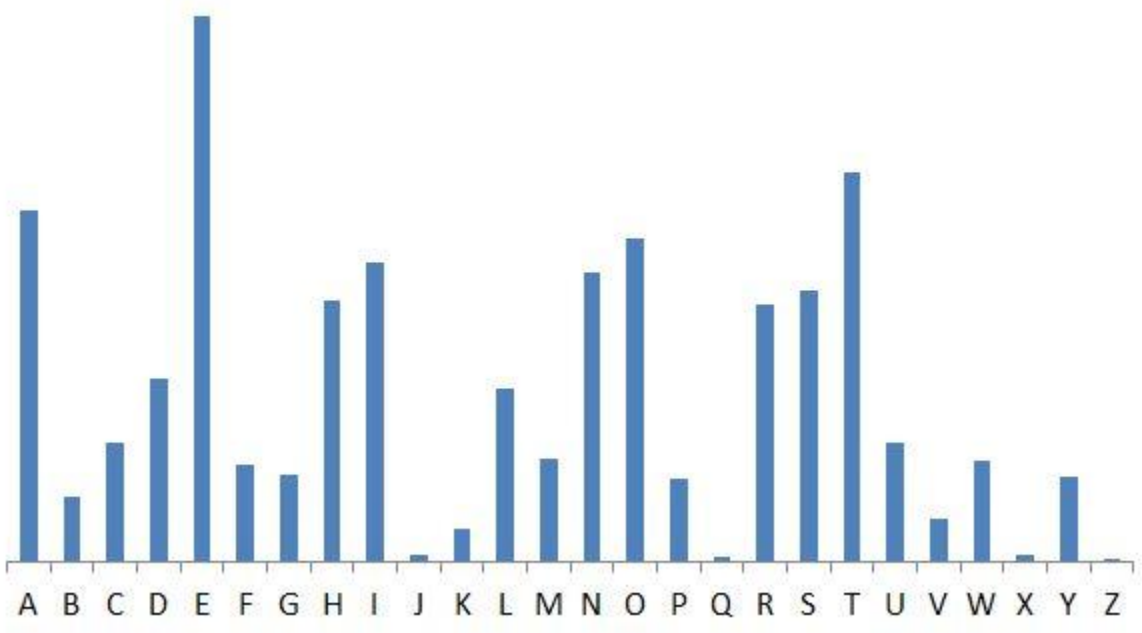
```
Исходный текст:   ATTACKATDAWN
Ключ:             LEMONLEMONLE
Зашифрованный текст:LXFOPVEFRNHR
```

Взлом шифра Виженера

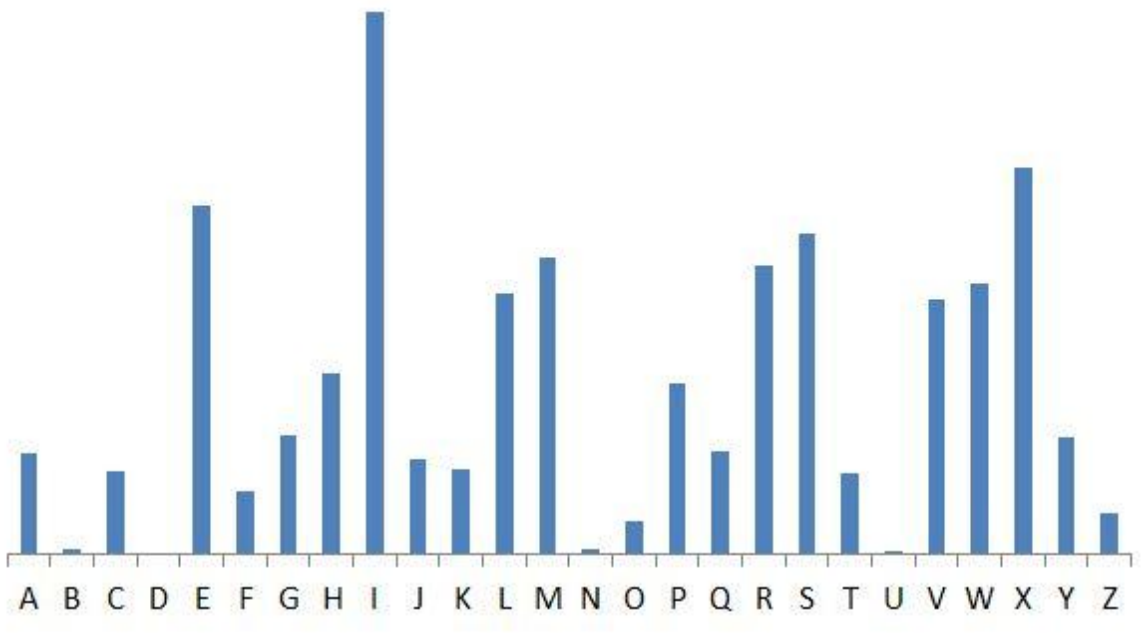
- Этапы:
- 1) поиск длины ключа N
- 2) взлом N различных шифров Цезаря

Взлом шифра Виженера

l	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ИС	0.038	0.043	0.047	0.043	0.038	**0.060**	0.037	0.042	0.049	0.043	0.038	**0.060**	0.036	0.041	0.048	0.042	0.039	**0.063**	0.038	0.043



Исходный алфавит



Алфавит со сдвигом 4

Шифр Плейфера

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

Исходное сообщение: IDIOCY OFTEN LOOKS LIKE INTELLIGENCE

Биграммы: ID IO CY OF TE NL OO KS LI KE IN TE LL IG EN CE

Заменяем повторы: ID IO CY OF TE NL OX OK SL IK EI NT EL LI GE NC E

Добиваем до биграмм: ID IO CY OF TE NL OX OK SL IK EI NT EL LI GE NC EX

Шифруем каждую биграмму:

- **Текст:** ID IO CY OF TE NL OX OK SL IK EI NT EL LI GE NC EX
- **Шифр:** KF FB BZ FM WA SP NV CF DU KD AG CE WP QD PN BS NE

До Второй мировой

TELEGRAM RECEIVED.

...LED
...tter 1-8-58
...rson, State Dept.
By Mack 9 Eckhoff Archivist
Date Oct. 22, 19[illegible]

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8387

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

MC

Check 3300

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

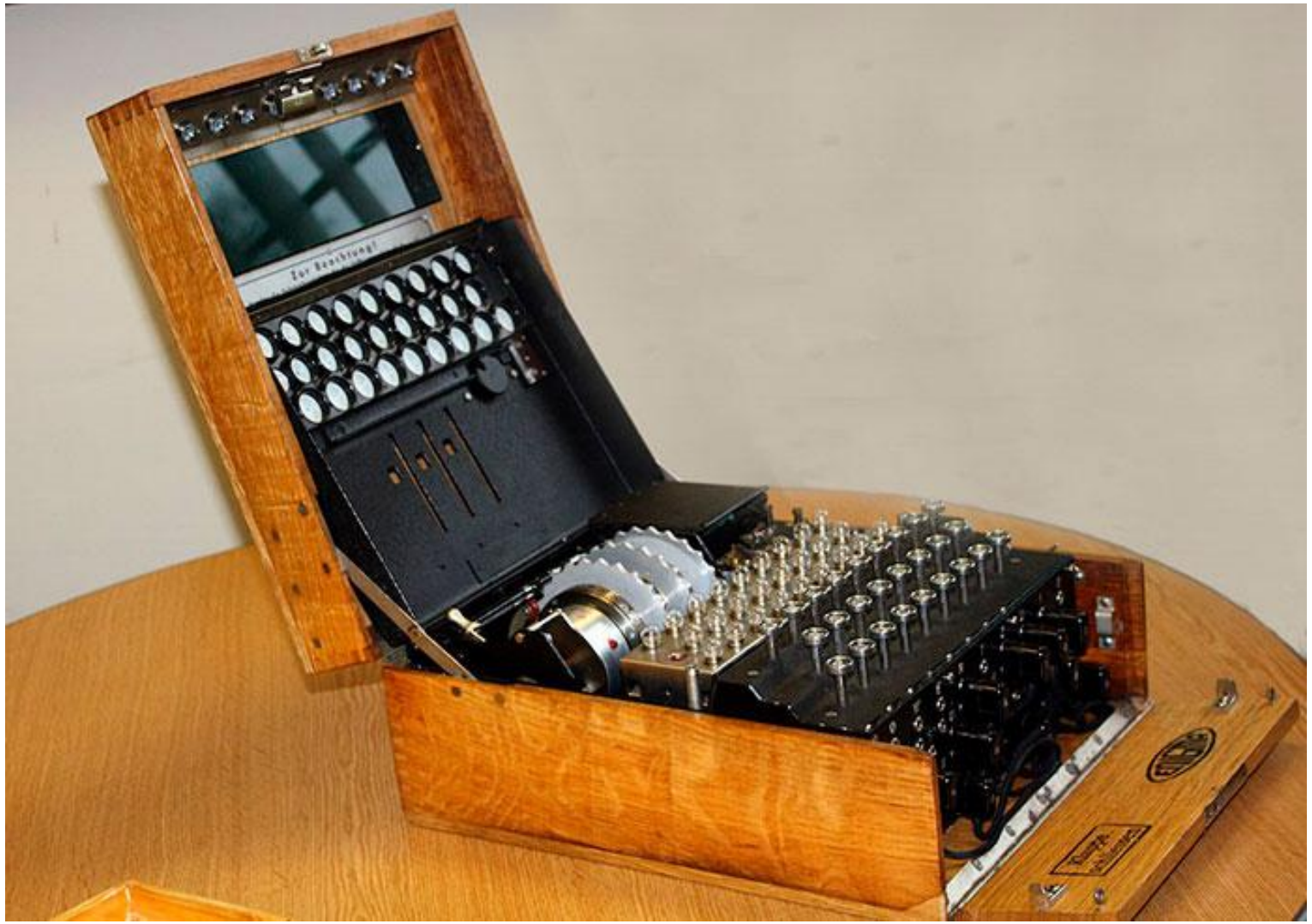
862.20212/324

Вторая мировая

Энигма

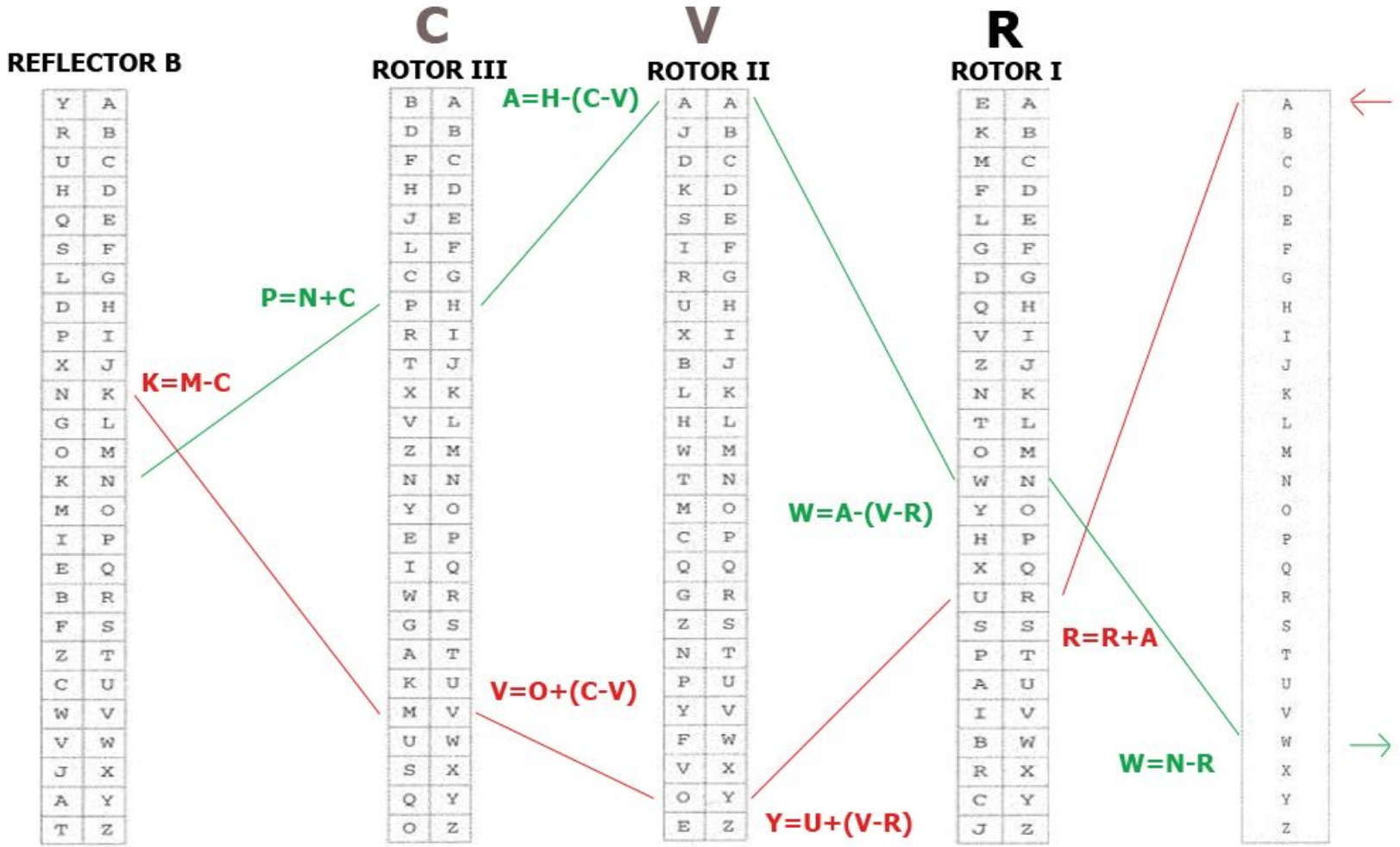
Машина Лоренца

Энигма



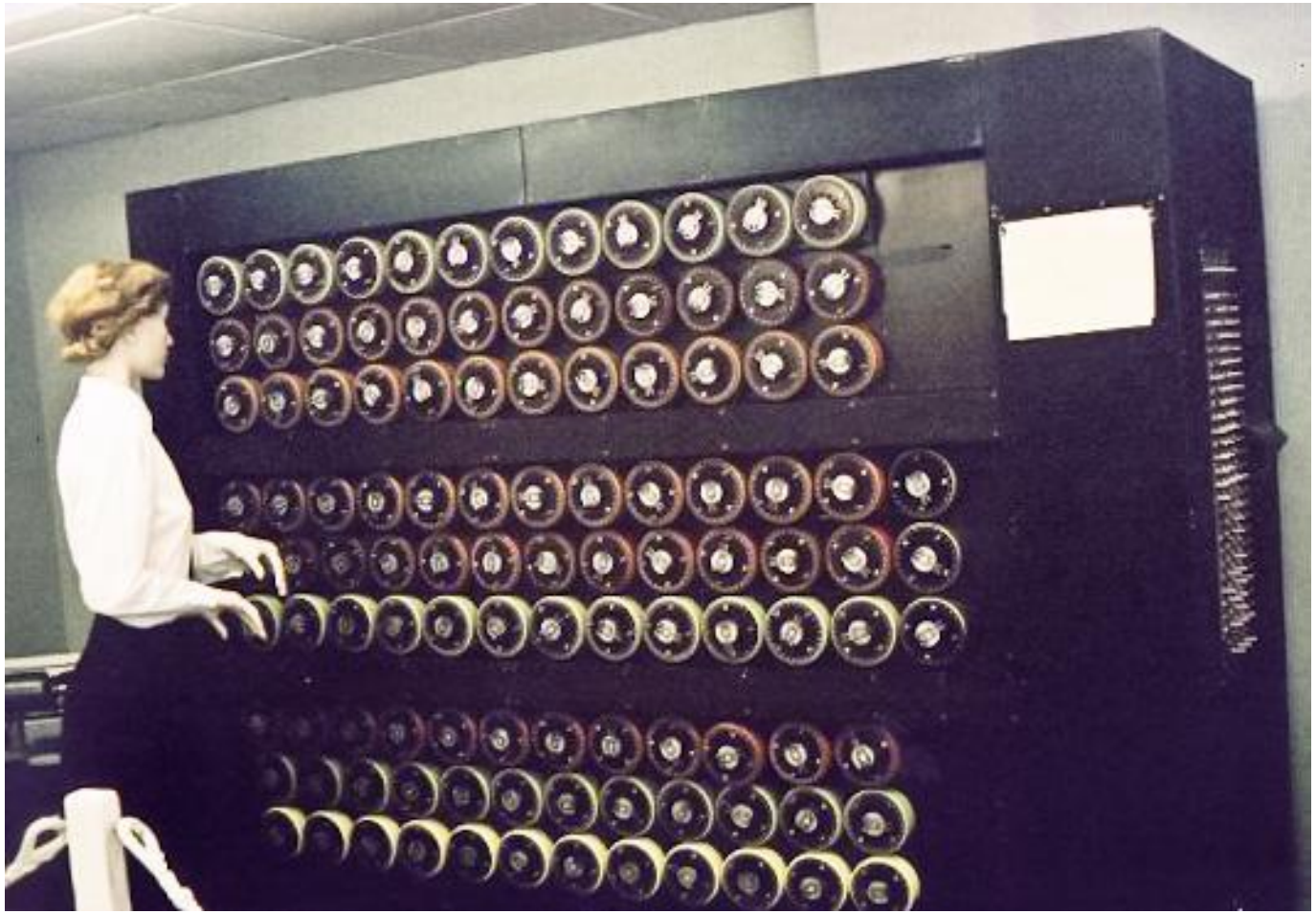
- 3-4 ротора
- Коммутационная панель
- Рефлектор
- Аксессуары

Алгоритм работы Энигмы

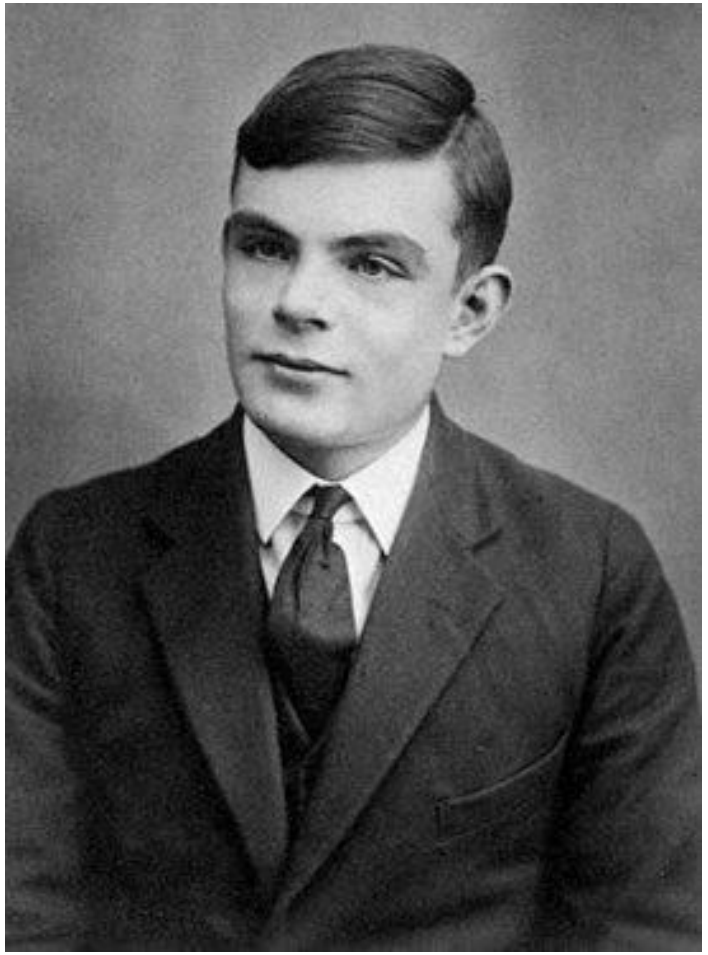


Блэтчли-парк

Bombe



BOMBE



Алан Тьюринг

Lorenz - принцип

Открытый текст ⊕ Ключ = Шифротекст

Шифротекст ⊕ Ключ = Открытый текст

ВХОД		ВЫХОД
A	***B***	***A⊕B***
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Шифрование Lorenz

Ключ =

Хи-ключ ⊕ Пси-Ключ

Номер диска	1	2	3	4	5	6	7	8	9	10	11	12
Количество контактов	43	47	51	53	59	37	61	41	31	29	26	23

Взлом алгоритма шифрования Lorenz

- Пусть Za и Zb - зашифрованный текст, Pa и Pb – открытый, K - ключ

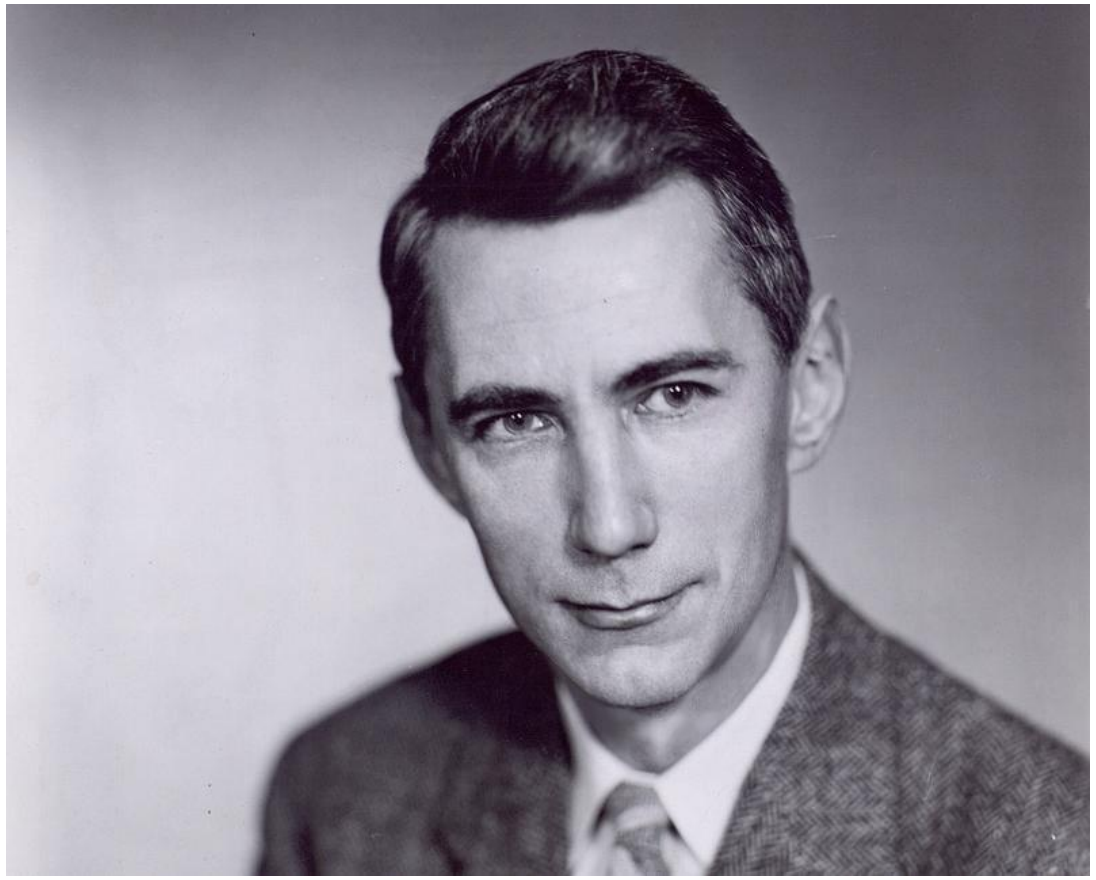
$Za \oplus Zb = Pa \oplus Pb$

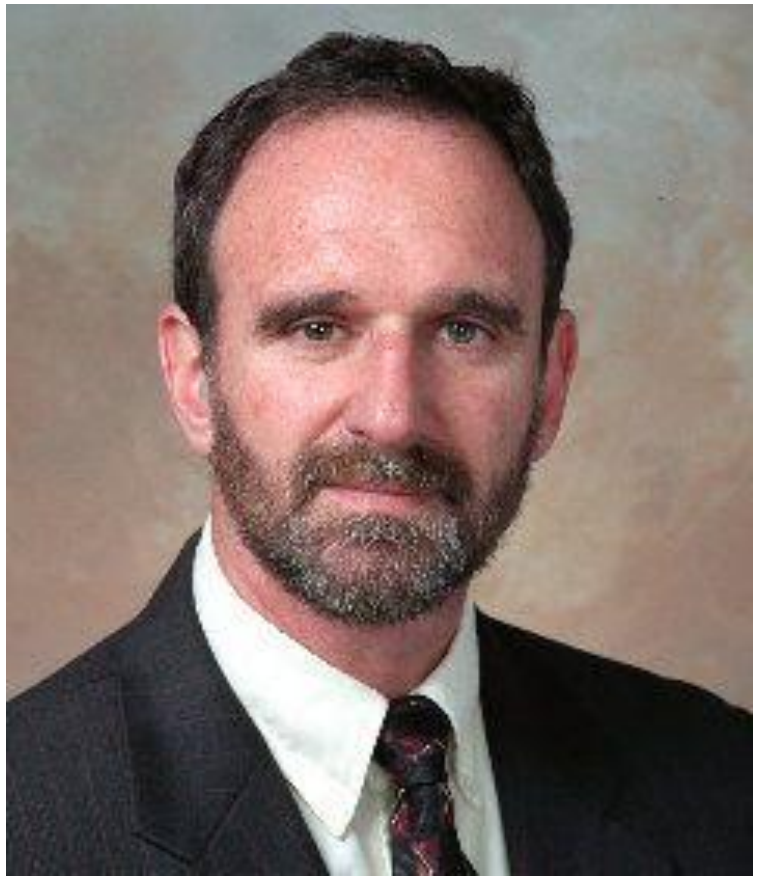
- Имея хотя бы по одной паре – открытый текст/шифротекст, получаем ключ:

$Za \oplus Pa = K$ или $Zb \oplus Pb = K$

МЕТОД КАСИСКИ – поиск повторов в шифротексте

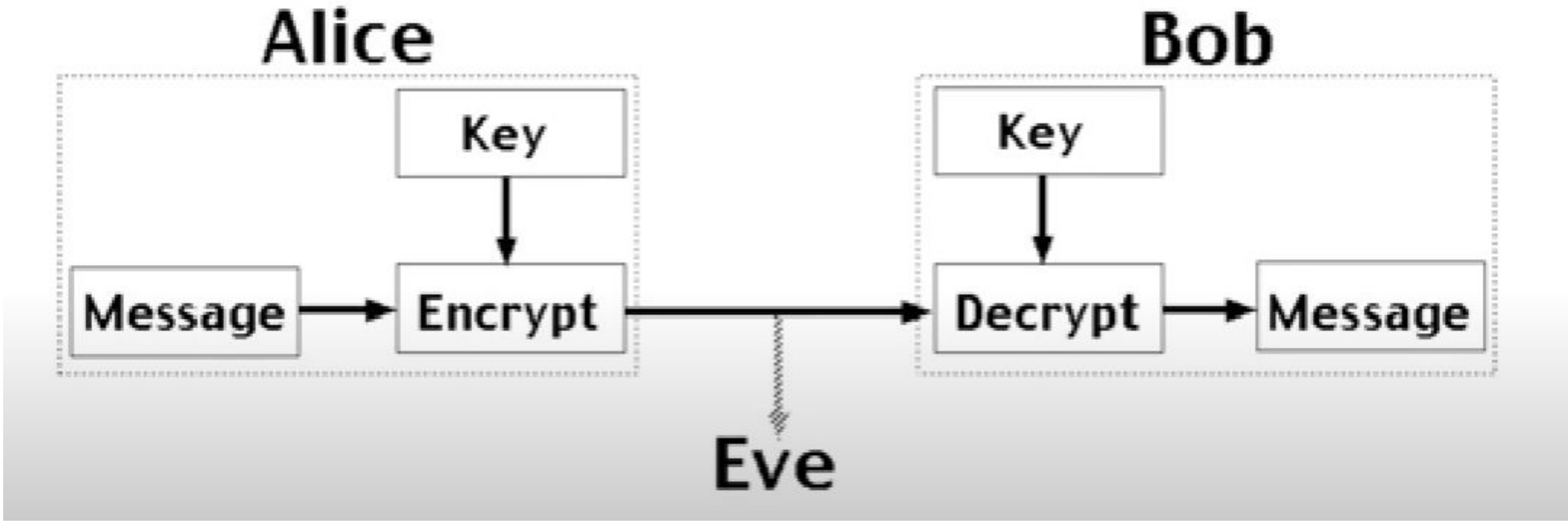
Математическая криптография





Вот они слева направа – Клод Шеннон, Уитфилд Диффи и Мартин Хеллман

Alice, Bob and Eve



Симметричные криптосистемы

- В симметричных криптосистемах для шифрования и дешифрования применяется один и тот же ключ

- Типичные представители:

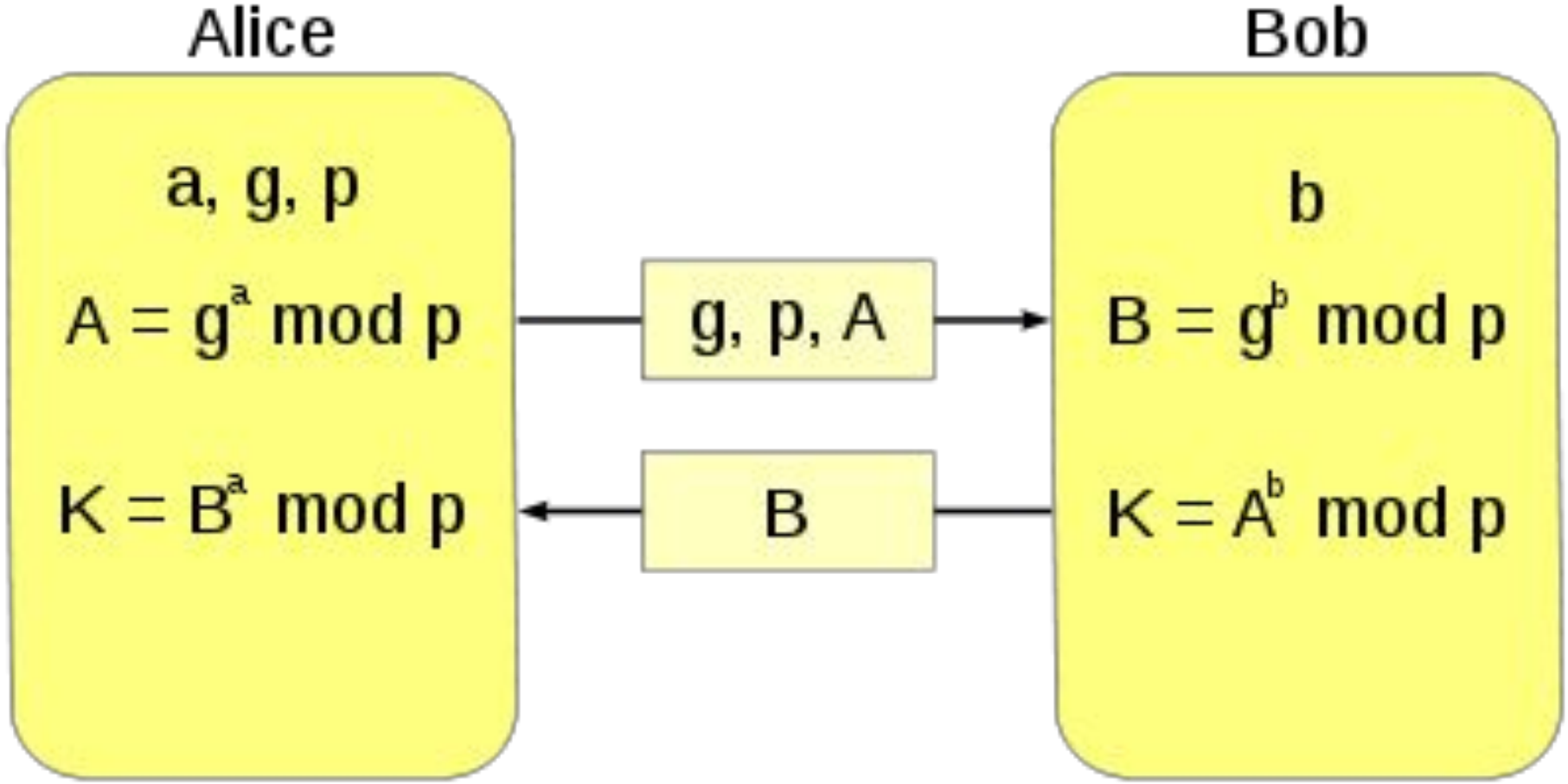
Простая перестановка

Перестановка по ключу

Уязвимости шифров перестановки

- Частотный анализ
- Атака словарем
- Для полиалфавитных шифров – метод Касиски
- Атаки на основе подобранного текста
- И множество других…

Протокол Диффи-Хеллмана

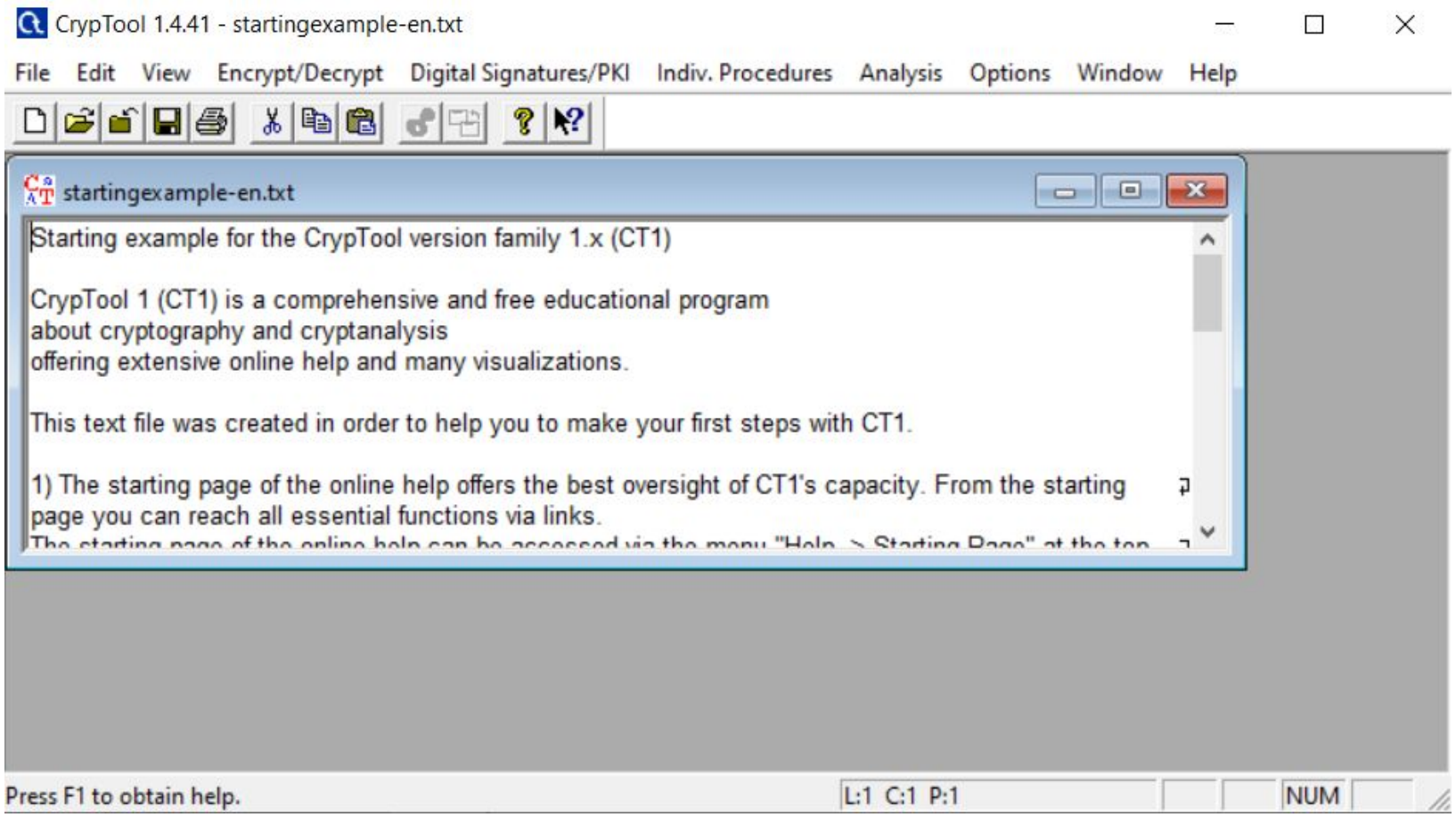


$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Тулзы

- CyberChef – очень большая база различных алгоритмов. Magic в помощь
- CrypTool – немного о нем далее
- Dcode.xyz – тоже большая база, на многие шифры осуществляет атаки грубой силой, вычисляет энтропию, даже определяет алгоритм шифрования – мощная вещь
- WinDecoder – очень красиво, быстро и наглядно ломает любой шифр простой замены. УРА!

Cryptool


CrypTool 1.4.41 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
Starting example for the CrypTool version family 1.x (CT1)
CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.
This text file was created in order to help you to make your first steps with CT1.
1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting
page you can reach all essential functions via links.
Press F1 to obtain help.
L:1 C:1 P:1
NUM