КРИПТОГРАФИЯ

Джгамая Ирина, 102нб

КРИПТОГРАФИЯ

(от греч. κρυπτός — скрытый и γράφω — пишу)

Криптография - наука о методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации.

КЛЮЧ

Ключ — параметр шифра, определяющий выбор конкретного преобразования данного текста.

В современных шифрах алгоритм шифрования известен, и криптографическая стойкость шифра целиком определяется секретностью ключа (Принцип Керкгоффса).

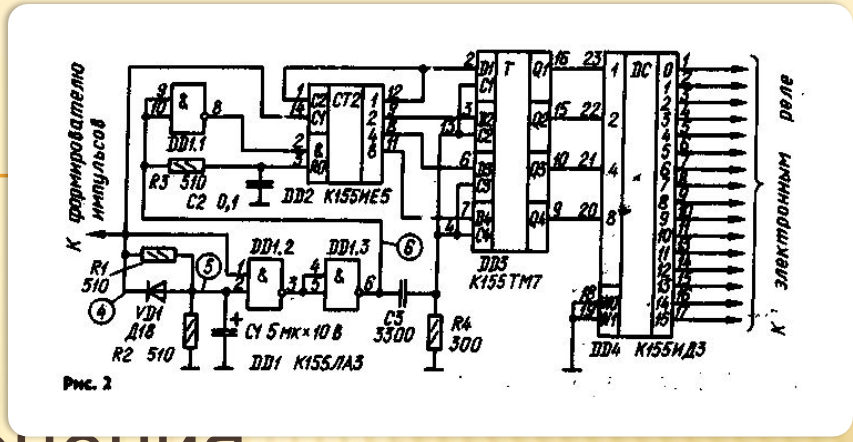


Рис. 2

Шифрование —применения криптографического преобразования открытого текста на основе алгоритма и ключа → шифрованный текст.

Расшифровывание — процесс нормального применение криптографического преобразования шифрованного текста в открытый.

ВИДЫ ТЕКСТА

Открытый (исходный) текст — данные передаваемые без использования криптографии.

Закрытый (шифрованный) текст — данные, полученные после применения криптосистемы с указанным ключом.

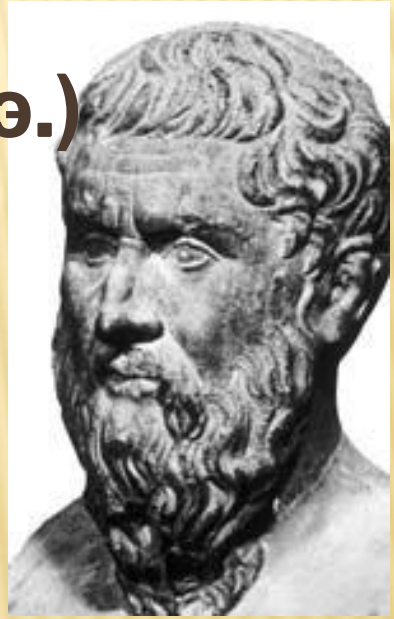
ИСТОРИЯ КРИПТОГРАФИИ

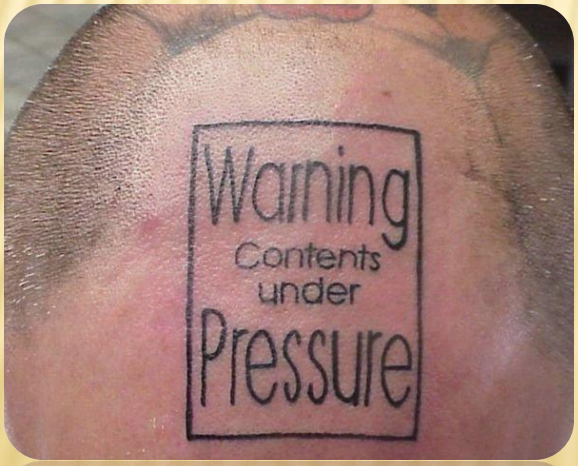
Способы тайной переписки были придуманы независимо во многих древних государствах, таких как Египет, Греция и Япония

Первые примеры криптогрфии

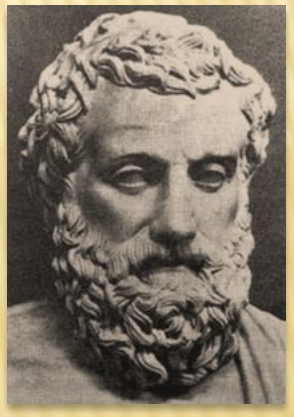
ТАТУИРОВКА

Геродот (484 до н. э. – 425 до н. э.) Татуировка, сделанная на обритой голове раба, скрытая под отросшими волосами.





СКИТАЛА (ШИФР ДРЕВНЕЙ СПАРТЫ)



Впервые скитала упоминается греческим поэтом Архилохом.

Скитала — это деревянный цилиндр.

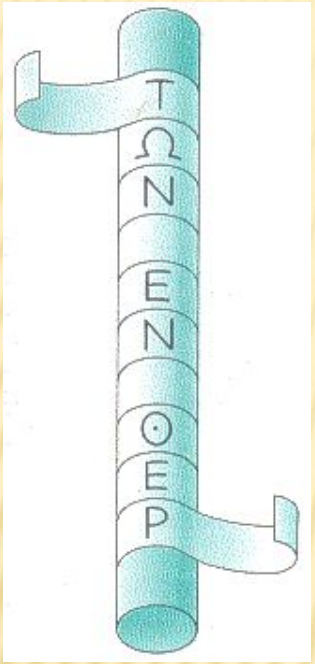
(от греч. Σκυτάλη – жезл)

Для криптосвязи требуется два цилиндра (одна скитала у того, кто будет отправляет сообщение, другая — у адресата.

Диаметр обоих должен быть строго одинаковым.

ПРИНЦИП ШИФРОВАНИЯ

1



2

Отправка по

3

	Н	А	С	Т	
	У	П	А	Й	
	Т	Е			

4

БИБЛИЯ

Книга пророка Иеремии (22,23): "...а царь *Сессаха* выпьет после них."

На языке оригинала мы имеем слово *Вавилон*.

АТБАШ

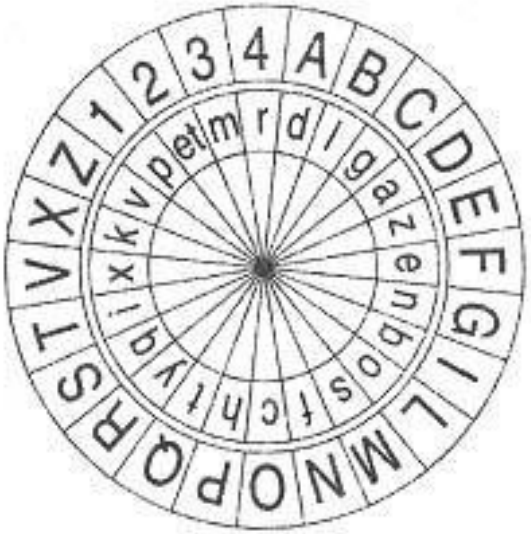
Исходный текст:
ABCDEFGHIJKLMNOPQRSTUV
WXYZ

Зашифрованный текст:
ZYXWVUTSRQPONMLKJIHGFE
DCBA

ДИСК С ШИФРОТЕКСТОМ АЛЬБЕРТИ

Леон Баттиста Альберти
(1404-1472)
«Трактат о шифрах»

Первая буква шифруется по первому шифроалфавиту, вторая по второму и т.д.



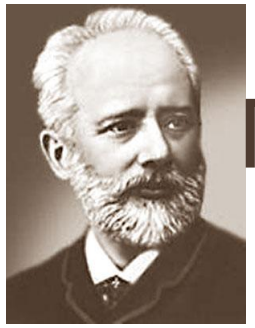
РЕШЕТКА КАРДАНУ

Джероламо Кардано (1501-1576)

«YOU KILL AT ONCE»

«I LOVE YOU. I HAVE YOU DEEP UNDER MY SKIN. MY LOVE LASTS FOREVER IN HYPERSPACE».

I		L	O	V	E		Y	O	U
I		H	A	V	E		Y	O	U
D	E	E	P		U	N	D	E	R
M	Y		S	K	I	N		M	Y
L	O	V	E		L	A	S	T	S
F	O	R	E	V	E	R		I	N
H	Y	P	E	R	S	P	A	C	E



ПЕТР И МОДЕСТ ЧАЙКОВСКИ

Замена каждой гласной русского языка на другую гласную, каждой согласной - на другую согласную:

«шыр-пир ю пяпюжгы зэлэмьгый гесрыг»

вместо:

«жил-был у бабушки серенький козлик».

ШИФР ВИЖЕНЕРА

	A	B	C	D	.	.	.	.	.	.	.	Z
A	A	B	C	D	.	.	.	.	.	.	.	Z
B	B	C	D	E	.	.	.	.	.	.	.	B
C	C	D	E	F	.	.	.	.	.	.	.	C
D	D	E	F	G	.	.	.	.	.	.	.	D
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
Z	Z	A	B	C	.	.	.	.	.	.	.	Y

Ключ - ABC

ключ	A B C A B C
открытый текст	D A N C E
шифрованный текст	

ключ	A B C A B C
открытый текст	D A N C E
шифрованный текст	D B P C F

	A	B	C	D	.	.	.	.	.	.	.	Z
A	A	B	C	D	.	.	.	.	.	.	.	Z
B	B	C	D	E	.	.	.	.	.	.	.	B
C	C	D	E	F	.	.	.	.	.	.	.	C
D	D	E	F	G	.	.	.	.	.	.	.	D
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
.	.	.	.	.								.
Z	Z	A	B	C	.	.	.	.	.	.	.	Y

произвольная буква

ключ	A D A N C E
открытый текст	D A N C E
шифрованный текст	

ЛИТЕРАТУРА О КРИПТОГРАФИИ

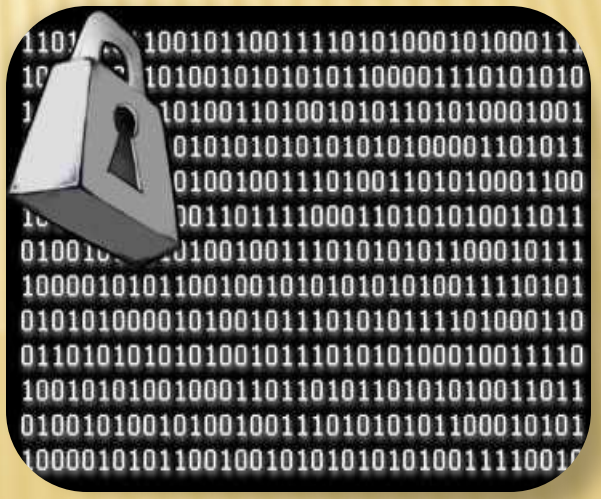
- **«Трактат о шифрах»,** Габриэль де Лавинд
- **«Энциклопедия всех наук»,** Шехаба Калкашанди (методы засекречивания содержания переписки)
- **«Интеллидженс сервис»,** Оливер Кромвель (раздел по дешифровке)
- **«Военная криптография»,** Огюст Кергоффс

...

ШИФР

(от араб. صِفْر , ṣifr «ноль», фр. chiffre «цифра»; родственно слову цифра)

Шифр — совокупность алгоритмов криптографических преобразований.




Шифр
симметричный
ассиметричный

КЛАССИЧЕСКИЕ ВИДЫ ШИФРОВАНИЯ

ПРОСТАЯ ЗАМЕНА

а б в г д е … я

1 2 3 4 5 6 … 33

Или:

A b c d t f …

! @ # $ % *…

Пример:

33 9 29 12 16 9 15 1 15 10 6

ЯЗЫКОЗНАНИЕ

ПЕРЕСТАНОВОЧНЫЙ ВИД

Буквы сообщения переставляются:

«помоги мне» → *«опомиг нме»*

«приду во вторник» → *«рпдиу ов твроинк»*

ЗАМЕЩАЮЩИЙ ВИД

Замены каждой буквы следующей за ней в алфавите:

«очень быстро» *«пшжоы вътусп»*

“good bye” *”hppe czf”*

ШИФР ЦЕЗАРЯ

Н → о п Р с ...

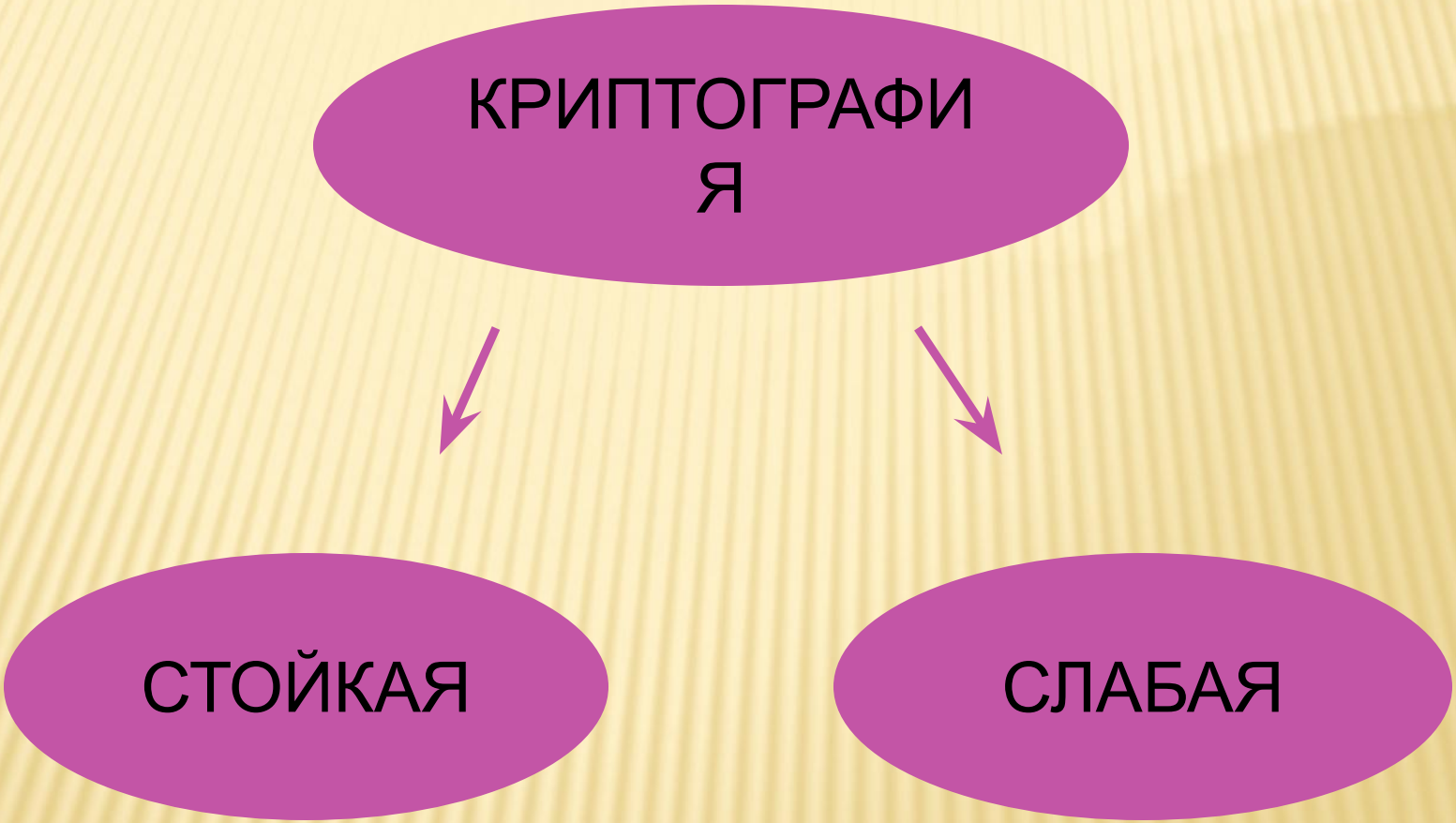
Юлий Цезарь использовал шифр со смещением 3 при связи со своими полководцами во время военных кампаний.

КРИПТОГРАФИЯ И ДРУГИЕ НАУКИ

До XX века криптография имела дело только с языковедческими образцами.

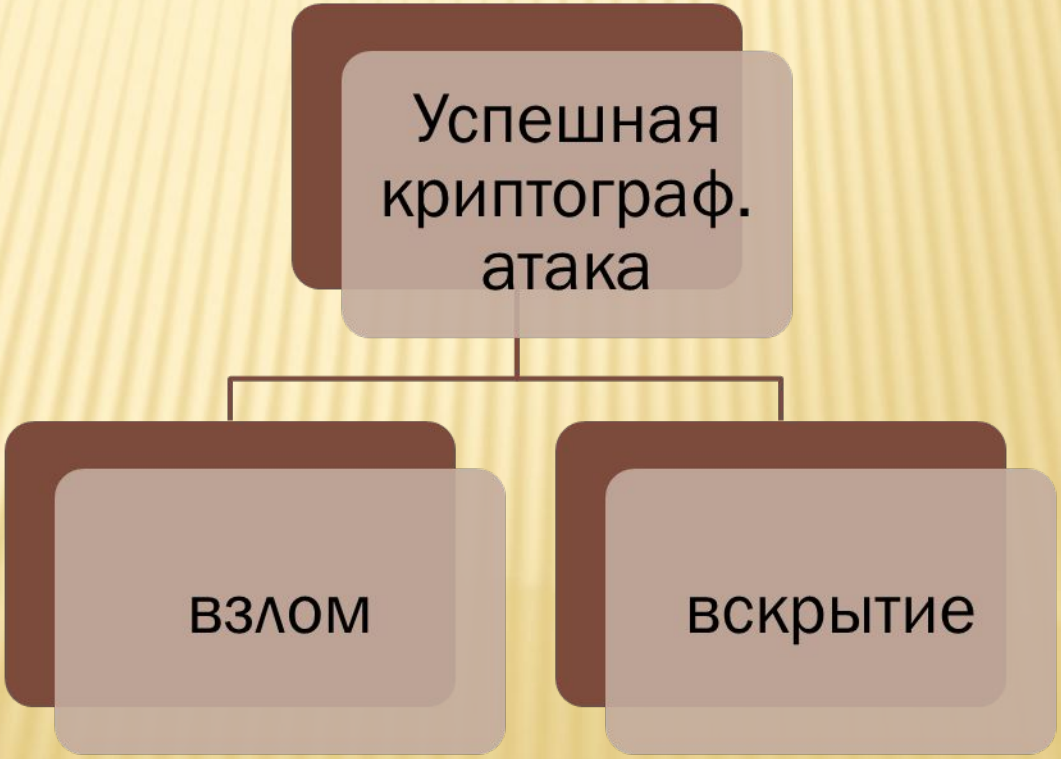
Сейчас:

- использование математики
- часть инженерного дела
- применение в криптографии квантовой физики


КРИПТОГРАФИЯ
СТОЙКАЯ
СЛАБАЯ

КРИПТОГРАФИЧЕСКАЯ АТАКА

Криптографическая атака – результаты криптоанализа конкретного шифра.

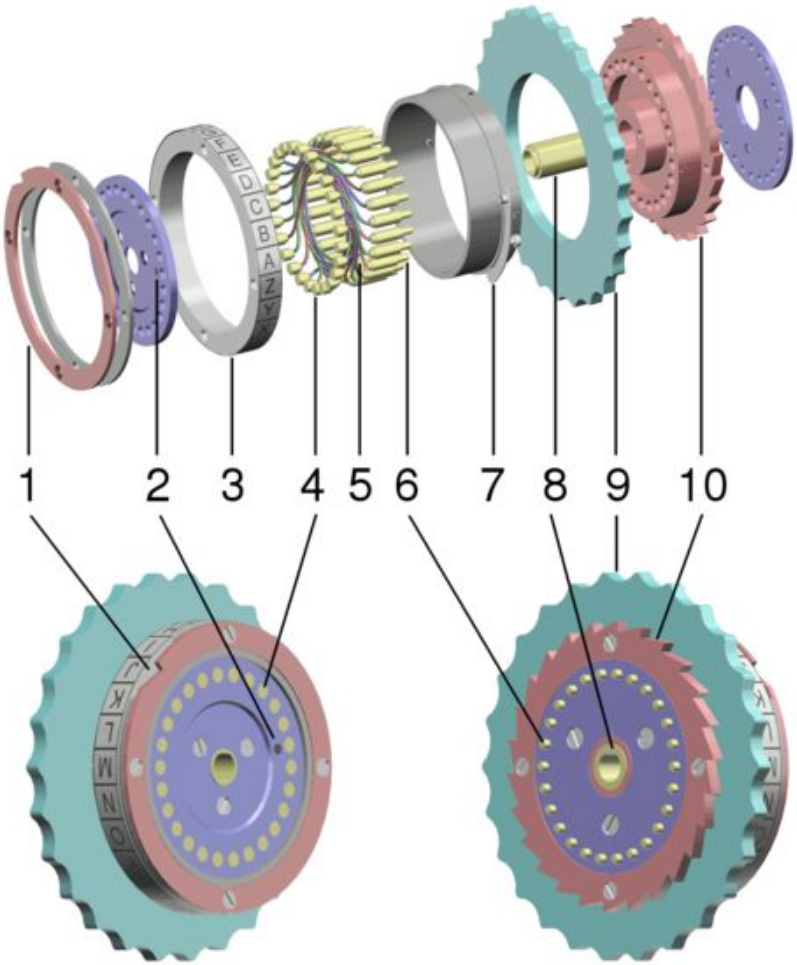


РОТОРНАЯ КРИПТОМАШИНА ENIGMA

Первая шифровальная машина.

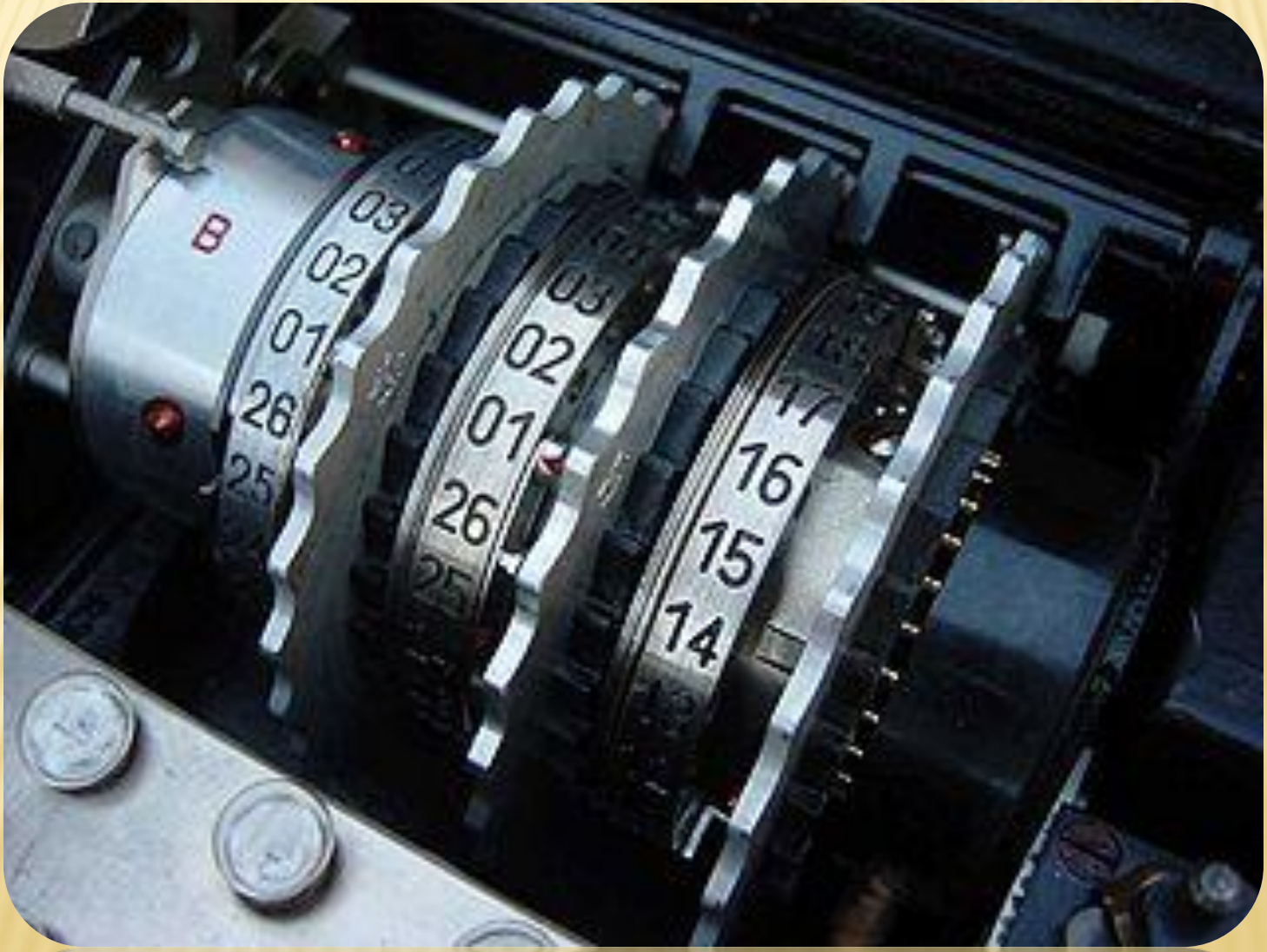
Использовалась германскими войсками с конца 1920-х годов до конца Второй мировой войны.

Ротор в разобранном виде



1. кольцо с выемками
2. маркирующая точка
3. для контакта «А»
4. алфавитное кольцо
5. залужённые контакты
6. электропроводка
7. штыревые контакты
8. пружинный рычаг для 9. настройки кольца
10. втулка
11. пальцевое кольцо

РОТОРЫ ЭНИГМЫ В СОБРАННОМ СОСТОЯНИИ

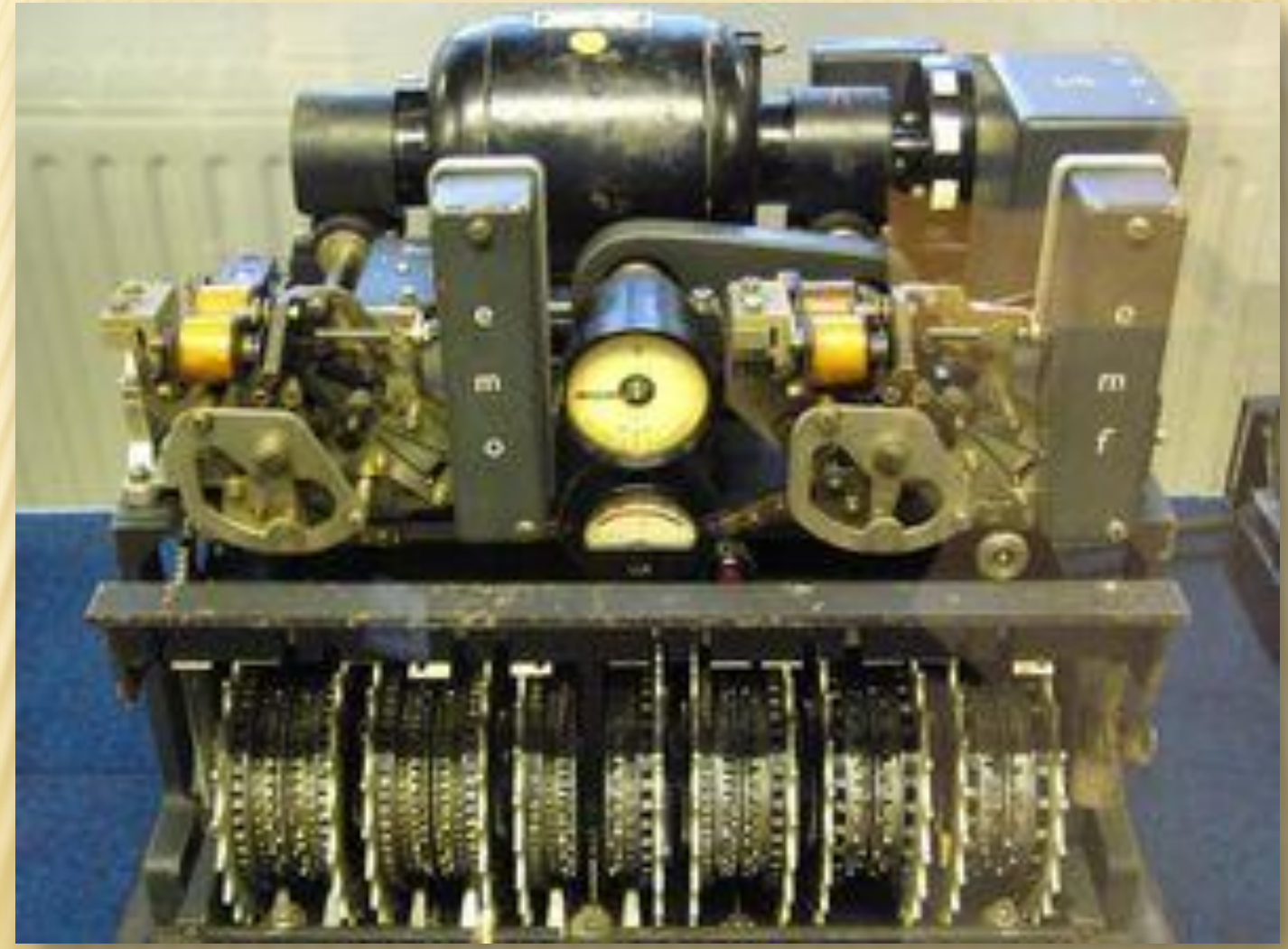


ПРИМЕРЫ ШИФРОВАНИЯ ЭНИГМЫ

E = PRMLUL − 1M − 1R − 1P − 1

E = P(ρiRρ − i)(ρjMρ − j)(ρkLρ − k)U(ρkL − 1ρ − k)(ρjM − 1ρ − j)(ρiR − 1ρ − i)P − 1

НЕМЕЦКАЯ КРИПТОМАШИНА LORENZ



КРИПТОАНАЛИЗ

Криптоанализ – наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого.

(Уильям Ф. Фридман, 1920)

Криптоаналитик — человек, создающий и применяющий методы криптоанализа.

КРИПТОЛОГИЯ

Криптология – наука, занимающаяся методами шифрования и дешифрования.

СОВРЕМЕННАЯ КРИПТОГРАФИЯ

Включает в себя:

- асимметричные криптосистемы
- системы электронной цифровой подписи (ЭЦП) хеш-функции
- управление ключами
- получение скрытой информации
- квантовую криптографию

СОВРЕМЕННАЯ КРИПТОГРАФИЯ

Распространенные алгоритмы:

- симметричные DES, Twofish, IDEA, и др.;
- асимметричные RSA и Elgamal
- хэш-функций MD4, MD5, ГОСТ Р 34.11-94.

RSA

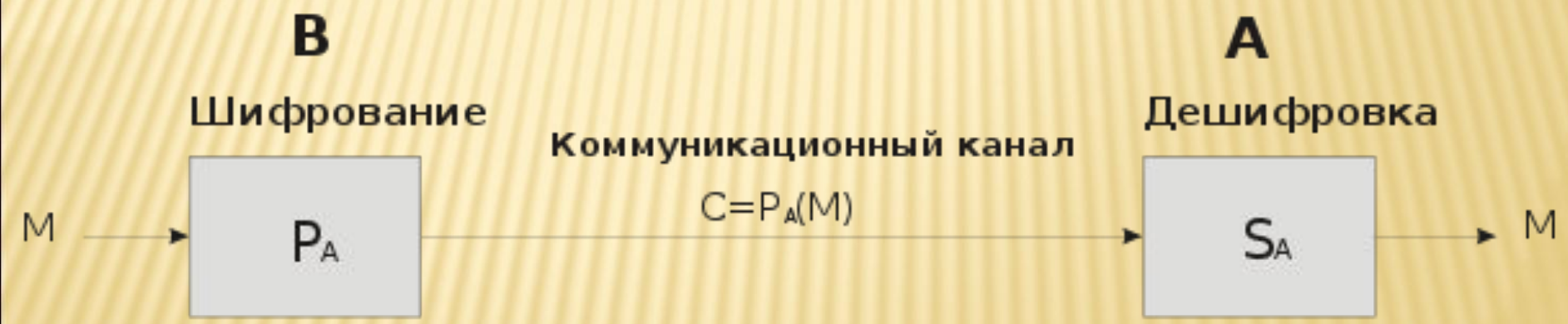
RSA (буквенная аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом.

СХЕМА RSA

A - отправитель

B - получатель

M - сообщение



Алгоритм:

- Взять *открытый ключ* (e, n) стороны A
- Взять открытый текст M
- Передать шифрованное сообщение:

$$P_A(M) = M^e \mod n \qquad (1)$$

Алгоритм:

- Принять зашифрованное сообщение C
- Применить свой *секретный ключ* (d, n) для расшифровки

$$S_A(C) = C^d \mod n \qquad (2)$$

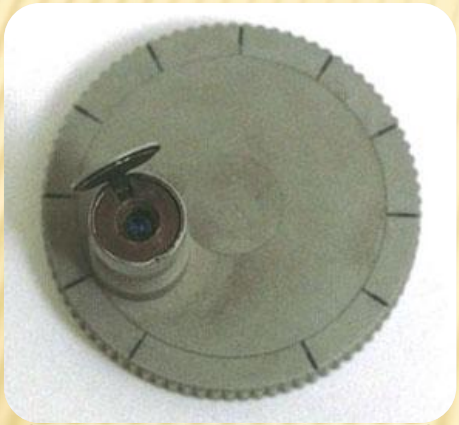
СОВРЕМЕННЫЕ СРЕДСТВА ШИФРОВАНИЯ

СИМПАТИЧЕСКИЕ ЧЕРНИЛА

Симпатические черни́ла — это чернила, записи которыми становятся видимыми только при определенных условиях.

МИКРОТОЧКИ

Микроточка — изображение, уменьшенное до такой степени, что невозможно обнаружить.



Фотокамера «Mark IV» для получения микроточек.

СПИСОК ПРОИЗВОДИТЕЛЕЙ, ИСПОЛЬЗУЮЩИХ МИКРОТОЧКИ:

- Audi
- BMW в Австралии
- Mitsubishi Ralliart
- Porsche
- Subaru
- Техмашимпорт (Techmashimport) в России
- Toyota

ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ

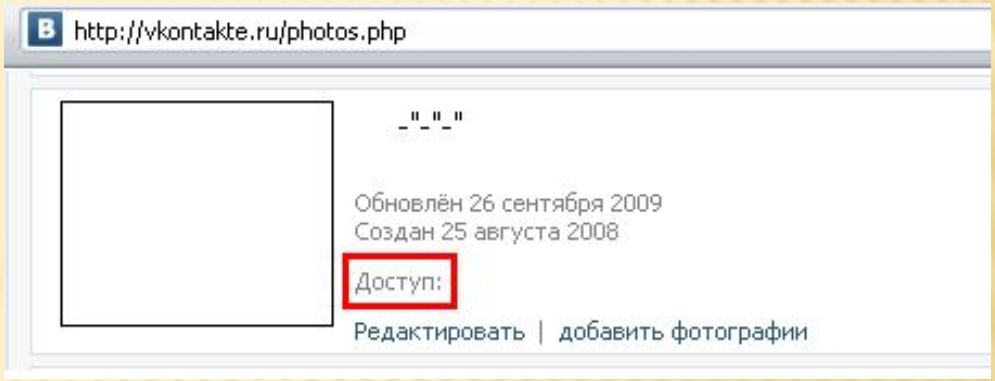
Цифровой водяной знак - это специальная метка, встраиваемая в цифровой контент с целью защиты авторских прав.

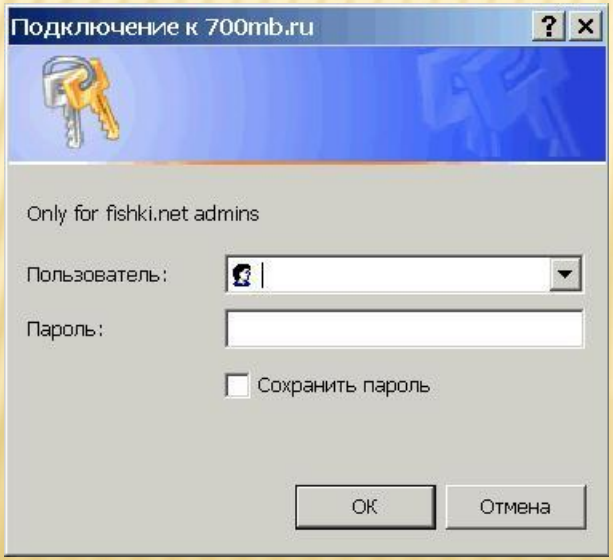
АКТУАЛЬНОСТЬ ШИФРОВАНИЯ СЕГОДНЯ

- широкое использование World Wide Web
- появление современных сверхмощных компьютеров

- расширилась сфера применения компьютерных сетей
- возможность дискредитации шифровых систем еще вчера считавшихся совершенно безопасными

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ СЕГОДНЯ





СПИСОК ЛИТЕРАТУРЫ

- Практическая криптография, А.В.Аграновский
- Англо-русский словарь-справочник по криптографии
- Алгоритмы шифрования, С. Панасенко
- Словарь криптографических терминов, Погорелова Б.А.
- http://crypto-r.narod.ru
- http://www.cryptopro.ru
- http://dic.academic.ru
- http://www.citforum.ru
- http://www.krugosvet.ru
- http://cryptolog.ru
- http://www.kpr-zgt.ru