КРИПТОГРАФИЯ

ОСНОВЫ ОСНОВ

КАМОЦКИЙ АНДРЕЙ

КРИПТОСРЕДА

14 МАРТА **2018**

SREDA
cryptofund

MOBILFON

КРИПТОГРАФИЯ

Криптогра́фия (криптос – скрытый, графо –пишу)
наука о:

- методах обеспечения конфиденциальности (невозможности прочтения информации посторонними)
- целостности данных (невозможности незамтного изменения информации)
- аутентификации (проверки подлинности авторства или иных свойств объекта)

Википедия

ИСТОРИЯ КРИПТОГРАФИИ

История криптографии насчитывает 4 тыс. лет

Основные периоды истории криптографии выделяются по технологиям используемых методов шифрования

ИСТОРИЯ КРИПТОГРАФИИ

I Период (с 3 тыс до н.э.)

Применялись моноалфавитные шрифты

Основной принцип – замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами

II Период (IX в н.э. до нач XX в.)

Применялись полиалфавитные шрифты

ИСТОРИЯ КРИПТОГРАФИИ

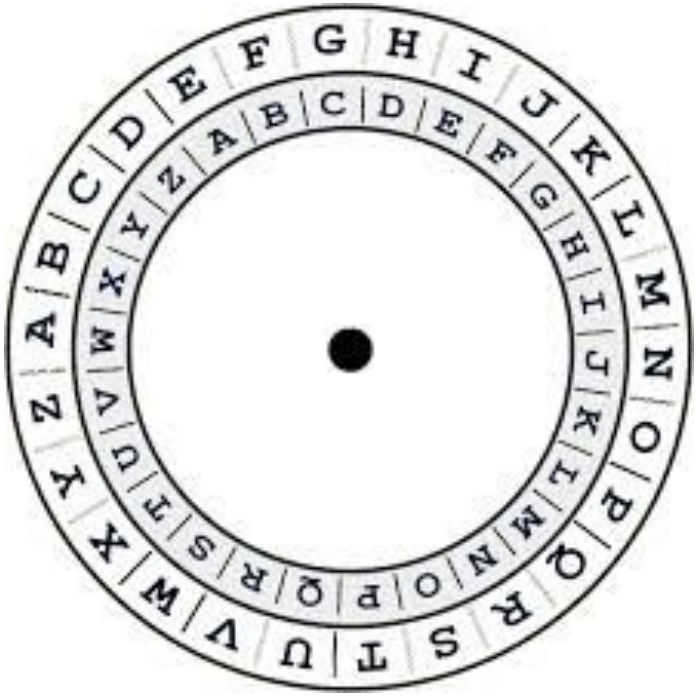
III Период (с нач. до сер. XX в.)

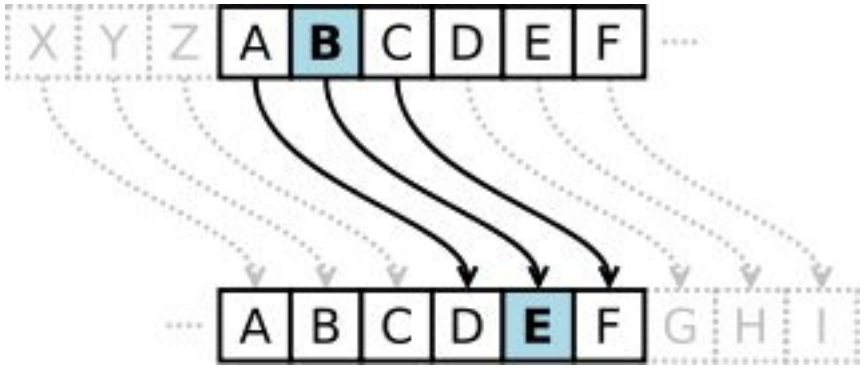
Внедрение электромеханических устройств в работы шифровальщиков

IV Период (с сер. XX в.)

Переход к математической криптографии

ШИФР ЦЕЗАРЯ (ШИФР СДВИГА)





Ключ:
Направление
Величина сдвига

SREDA = ONAZW

ПАРНЫЙ ШИФР

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

SREDA = NLUXV

ШИФР «4 КВАДРАТА»

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

SR=ON, ED=RP, AA=SC

SREDA = ONRPS

ШИФР ПЕРЕСТАНОВКОЙ

2	4	1	5	3
К	Р	И	П	Т
О	Ф	О	Н	Д
С	Р	Е	Д	А

1	2	3	4	5
И	К	Т	Р	П
О	О	Д	Ф	Н
Е	С	А	Р	Д

КЛЮЧ - 24153

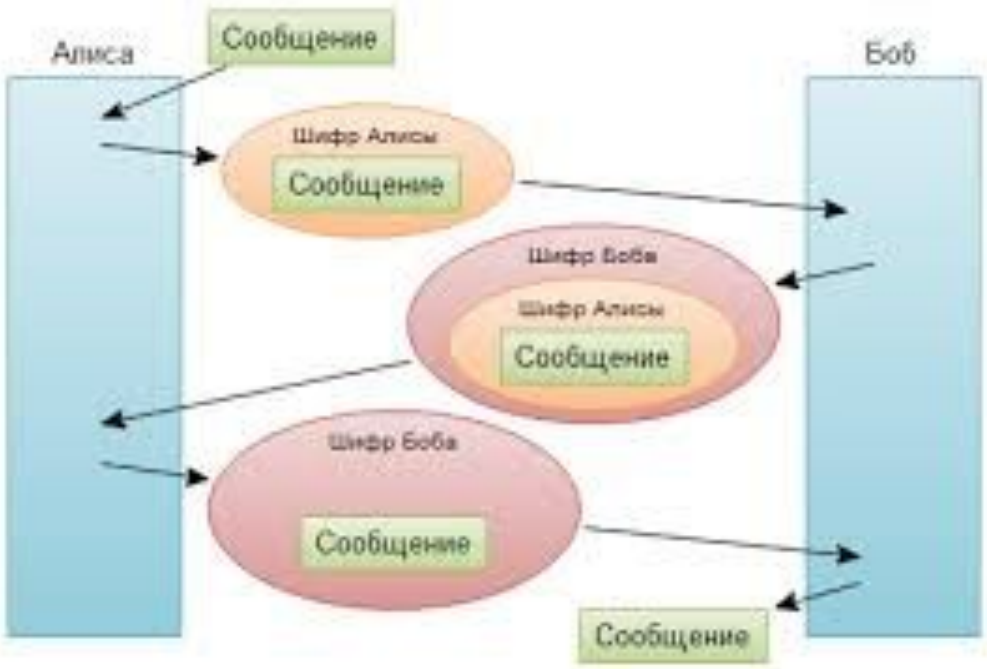
НЕДОСТАТКИ ШИФРОВ

НУЖНО ЗНАТЬ КЛЮЧ

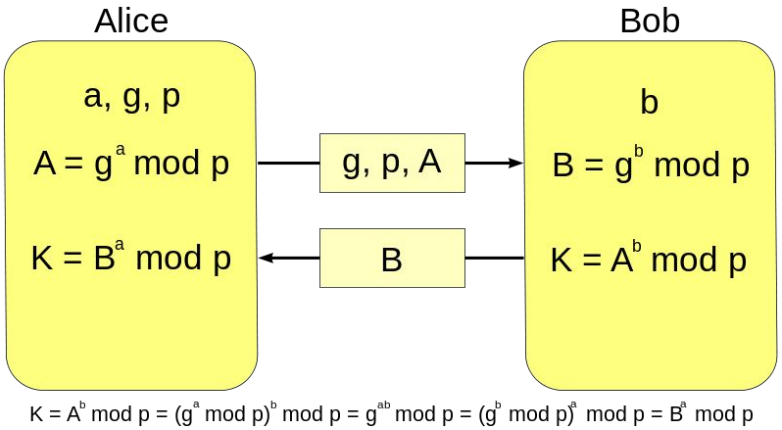
ОТНОСИТЕЛЬНО ЛЕГКО ПОДОБРАТЬ

ЧЕМ БОЛЕЕ КРИПТОСТОЙКИЙ ШИФР, ТЕМ СЛОЖНЕЕ С НИМ РАБОТАТЬ

АССИМЕТРИЧНОЕ ШИФРОВАНИЕ



ПРОТОКОЛ ДИФФИ-ХЕЛМАНА **(1976)**



Каждая сторона

1. Генерирует случайное число *a*
2. Устанавливают открытые параметры *p* и *g*
3. Вычисляет открытый ключ A
4. Обменивается открытыми ключами
5. Вычисляет открытый ключ *K*.

K получается равным с обеих сторон

На практике:

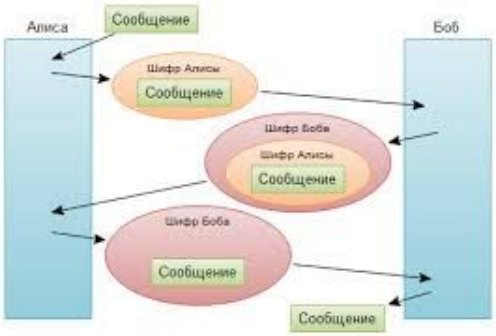
a, b - 10^{100}

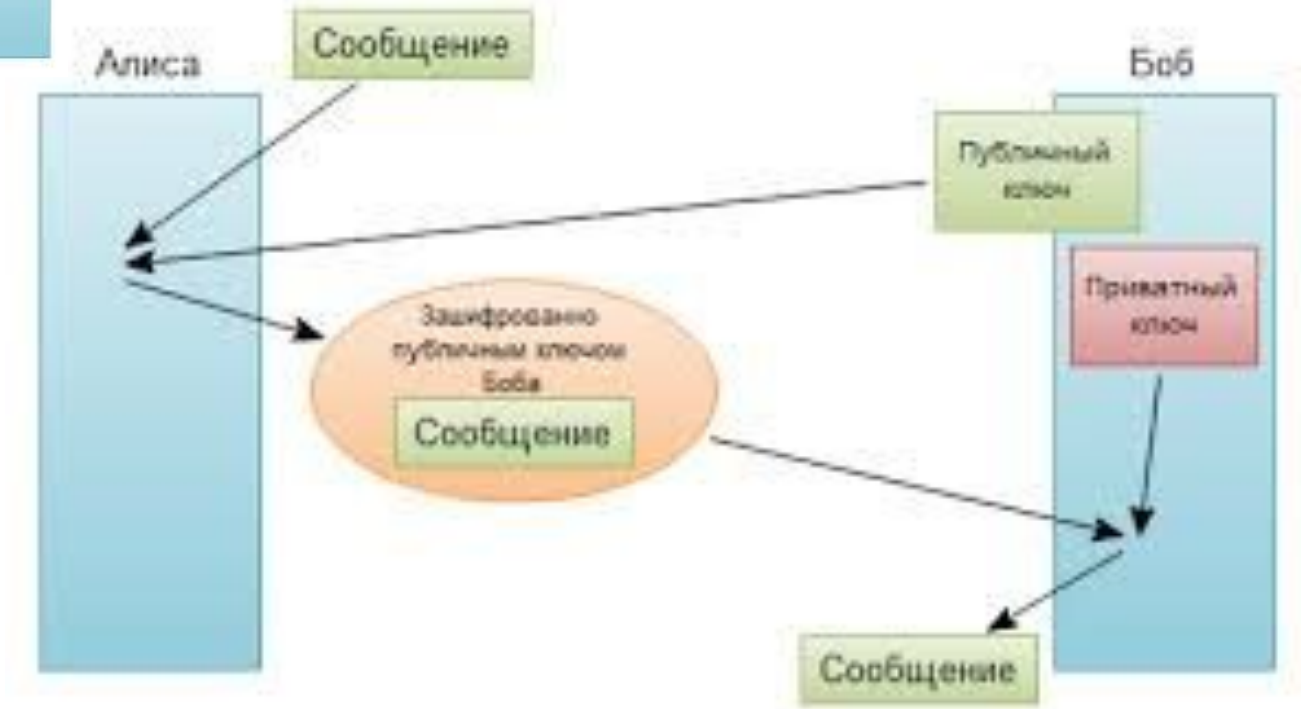
P - 10^{300}

K получается равным с обеих сторон, потому что:

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

В РЕАЛЬНОМ МИРЕ





ПРИМЕНЕНИЕ КРИПТОГРАФИИ

1. **Цифровая подпись**
2. **Передача информации**
3. **Сайты**
4. **Платежи**
5. **Связь**
6. **Криптовалюты**

И др.

КРИПТОВАЛЮТА

Криптовалюта – разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах.

Информация о транзакциях обычно не шифруется и доступна в открытом виде. Для обеспечения неизменности базы цепочки блоков транзакций используются элементы криптографии

ЕЩЕ...

Blockchain

Hash – функция

Подтверждение транзакций

СПАСИБО ЗА ВНИМАНИЕ!

@Andrewmf

facebook.com/a.kamotskiy

Камоцкий Андрей

КриптоСреда

14 марта 2018