Исторические шифры

Курс криптографии
кафедра БИТ
ИТМО

Содержание

- Введение, основные понятия
- Докомпьютерные шифры – **шифр Цезаря, шифр замены, «Энигма»**.
- Ненадежность этих шифров.
- Понятия **перестановки и замены** как основных компонентов шифра.
- Примеры атак на шифры.

Введение – основные понятия

Криптография ("kryptos" – тайный, "grapho" – пишу = "тайнопись")

Криптография - это наука о методах обеспечения конфиденциальности (невозможность прочтения информации посторонним лицом) и аутентичности информации (целостность и подлинность авторства, невозможность отказа от авторства)

Шифрование – процесс преобразования открытого текста с помощью криптографического алгоритма и ключа в зашифрованный текст

Стеганогра́фия (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.

Термин был введен в 1499 году Иоганн Тритемий в своем трактате «Стеганография».

Введение - обозначения

Процесс шифрования $C = E_k(m)$

Процесс расшифровывания $m = D_k(C)$

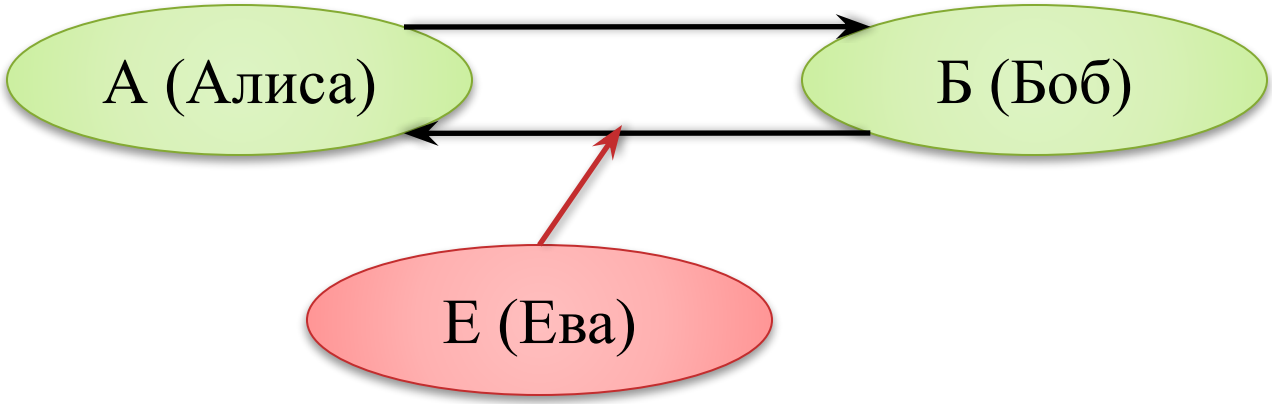
E – Encrypt - шифрующая функция

D – Decrypt - расшифровывающая функция

C – Cipher - шифротекст

m – message - открытый текст

k – key - секретный ключ



Введение

The Eavesdropper
(подслушивающий)

Шифры – сдвига и замены

- **Шифр сдвига**

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	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

hello □ KHOOR

Шифр Цезаря – сдвиг с ключом k = 3 (Недостаток ???)

- **Шифр замены**

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

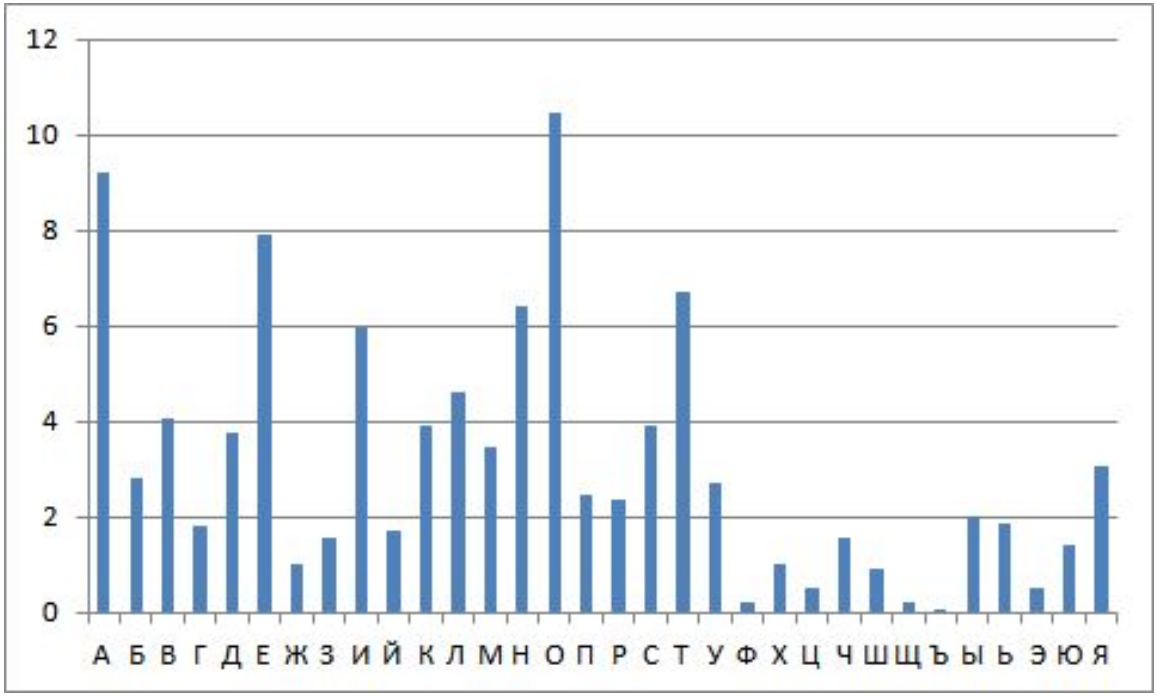
hello □ QBTTG

Число возможных ключей 26!

Шифры - моноалфавитные

Шифры сдвига и замены – *моноалфавитные шифры*

Метод взлома – частотный анализ



Шифры – шифр Виженера

полиалфавитный шифр замены

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

hello□ QNTKG (a не QBTTG) (Недостаток ???)

Шифр Виженера

	t	h	i	s	i	s	a	t	e	s	t	m	e	s	s	a	g	e
+	s	e	s	a	m	e	s	e	s	a	m	e	s	e	s	a	m	e
=	**L**	**L**	**A**	**S**	**U**	**W**	**S**	**X**	**W**	**S**	**F**	**Q**	**W**	**W**	**K**	**A**	**S**	**L**

Метод взлома – **тест Казисского**

Перестановочные шифры

Фиксируется перестановка

$\sigma =$

1	2	3	4	5
2	4	1	3	5

1. *once upon a time there was a little girl called Snow White*
2. *onceu ponat imeth erewa salit tlegi rlcal ledsn owwhi te*
3. *coenu npaot eitmh eewra lsiat etgli crall dlsen wohwi et*
4. *Coenunpaoteitmheewralsiatetglicralldlsenwohwiet*

Метод взлома – **атака с выбором открытого текста**

a	b	c	d	e	f	g	h	i	j	…
C	A	D	B	E	H	F	I	G	J	…

1	2	3	4	5	6	7	8	9	10	…
2	4	1	3	5	7	9	6	8	10	…

$\Rightarrow$ n = 5

Роторные машины

1. Берется полый диск, с нанесенными с двух сторон контактами- алфавит открытого и шифрованного текста
2. Контакты соединены между собой по некоторой подстановке называемой коммутацией диска.
3. При замене углового положения диска меняется и соответствующая замена на сопряженную подстановку.

1 буква

a	b	c	d	e	f	g	h	…
P	Q	G	H	U	I	K	L	…

2 буква

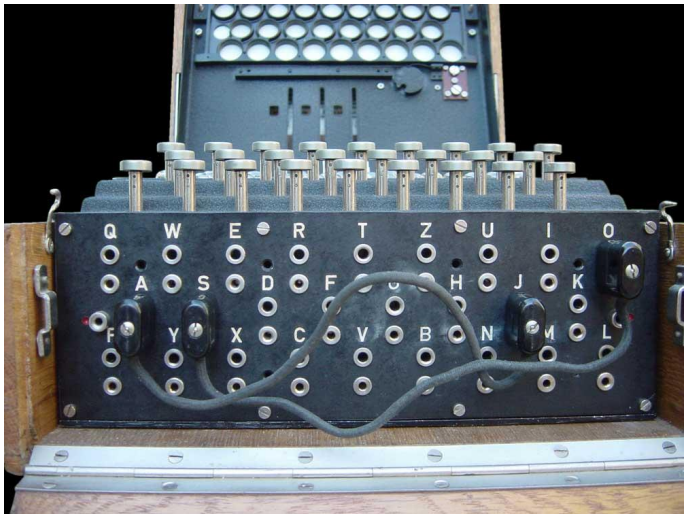
a	b	c	d	e	f	g	h	…
Q	G	H	U	I	K	L	A	…

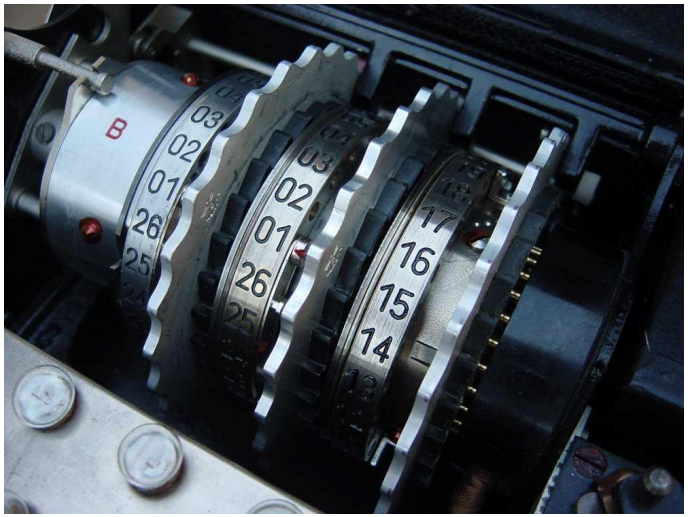
и т.д.

«Энигма»

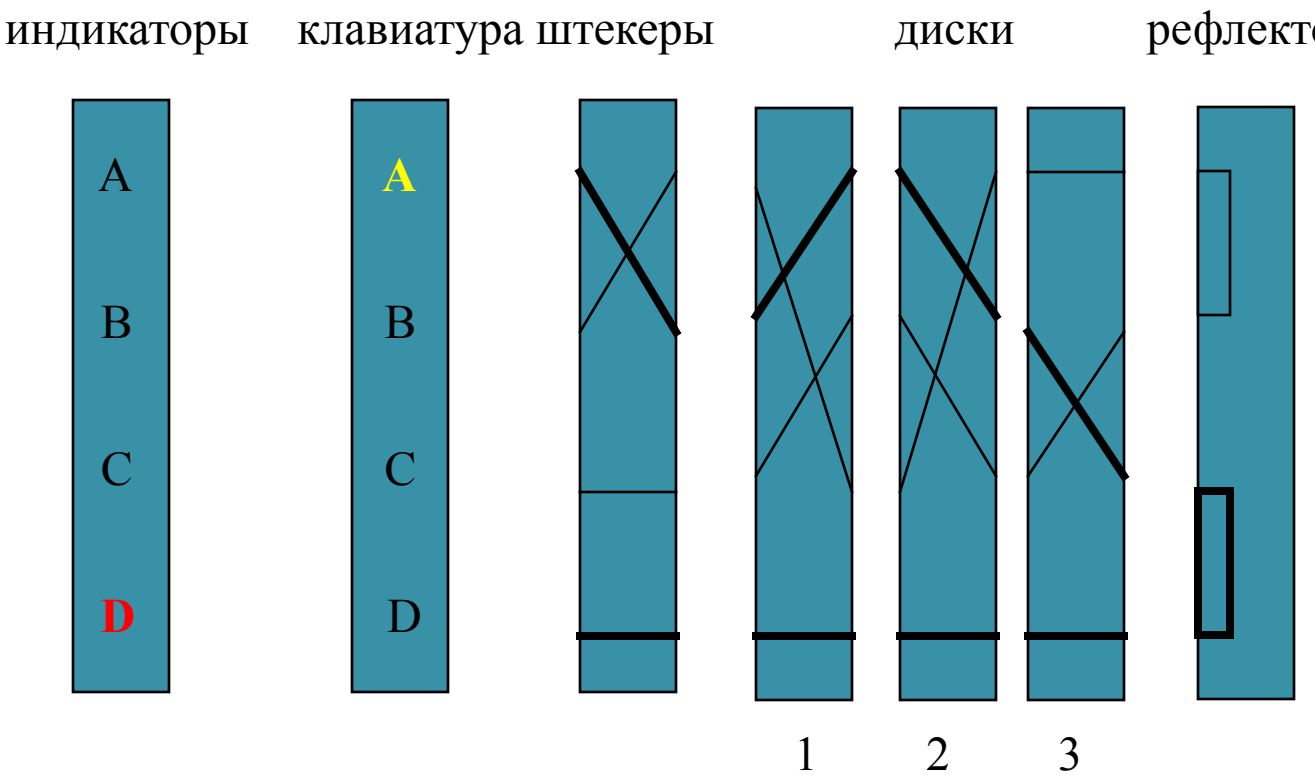
"Энигма" в первоначальном промышленном варианте фирмы «Сименс», созданном берлинским инженером Артуром Кирхом, представляла собой четыре вращающихся на одной оси барабана, что обеспечивало более миллиона вариантов ключа, которые определялись текущим положением барабанов. На каждой стороне барабана по окружности располагались 26 электрических контактов (сколько букв в алфавите). Контакты с обеих сторон барабана соединялись попарно случайным образом 26 проводами, формировавшими замену символов. Колеса складывались вместе, и их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов сквозь весь пакет колес.

«Энигма»


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


B
03 02 01 26 25
03 02 01 26 25
17 16 15 14

«Энигма»


индикаторы
клавиатура
штекеры
диски
рефлектор
A
B
C
D
A
B
C
D
1
2
3

«Энигма»

Ключ:

1. Расположение штекеров
2. Коммутационные диски и их компоновка
3. Позиции колец
4. Начальное угловое положение дисков

Перед передачей приходил **сеансовый ключ**.

Основные компоненты шифра

- **Замены** (сдвиг – частный случай замены) **(substitution)**
- **Перестановки (permutation)**

Алгоритмы

Def. Алгоритмы – *симметричными криптосистемами* или *криптосистемами с секретным ключом* если процесс шифрования и расшифровывания используют один ключ.

Def. Алгоритмы – *асимметричными криптосистемами* или *криптосистемами с открытым ключом* если процесс шифрования и расшифровывания используют два различных ключа.