



Шифры

Лекция 1:

- *Сцираль* - маршрутная перестановка
- *Диск Энея*
- *Квадрат Полибия* - простая замена

Лекция 2:

- *ATBASH* - запись основывалась на алфавите в обратном порядке
- *Линейка Энея* - простая замена
- *Шифр Цезаря* - простая замена
- *Цифровая тайнопись* - замена обычных букв иными на основе их численного значения

Лекция 3:

- *Колонная перестановка* - запись в таблицу и чтение по колонкам сверху вниз слева направо - маршрутная перестановка
- *Обратный порядок записи*
- *Редукция гласных*
- *Магические квадраты* - размера $n \times n$, буквы открытого текста записываются в квадрат в соответствии с нумерацией его клеток - маршрутная перестановка
- *Лозунговый шифр* - под алфавитом пишутся различные буквы лозунга, а затем буквы, не появившиеся в лозунге, далее происходит замена - простая замена
- *Диск Альберти режим 1* - первая буква сама в себя, сдвиг на 1 внутреннего диска, вторая буква открытого текста отыскивается на внешнем диске и заменяется на букву внутреннего диска и тд

- *Диск Альберти режим 2* - первая буква сообщения на внутреннем диске ставится напротив буквы "А" на внешнем. Первая буква сообщения ищется на внешнем диске и заменяется на букву внутреннего диска, далее сдвиг на 1 и тд
- *Диск Альберти режим 3* - индикаторная буква устанавливается напротив буквы "А". Первая буква сообщения ищется на внешнем диске и заменяется на букву внутреннего диска, далее сдвиг на 1 и тд
- *Диск Альберти режим 4* - произвольная буква устанавливается напротив буквы "А" и записывается в виде заглавной, несколько символов шифруются без сдвига внутреннего диска. Далее в шифртексте снова ставится заглавная буква напротив буквы "А", задающая новое положение диска и тд
- *Диск Альберти режим 5* - выбирается пароль, первая буква пароля совмещается с буквой "А" внешнего текста, шифруется первая буква открытого текста. Далее с буквой "А" совмещается вторая буква пароля и шифруется вторая буква текста и тд

Лекция 4:

- *Миланский ключ* - гласным буквам ставилось в соответствии несколько знаков шифруемого алфавита, число которых пропорционально частоте встречаемости буквы в открытом тексте
- *Омофонная замена* - не является многоалфавитным шифром
- *Шифр Марии Стюарт*
- *Таблица Тритемия* - многоалфавитный шифр - состоит из периодически повторяющейся последовательности простых замен

Исходное сообщение:
«Panem et circenses»
 («Хлеба и зрелищ», Ювенал, римский поэт-сатирик)

Шифртекст:
«РВРНQ КА КRBNQAGT!»

- **Решётка Кардано** - **квадратная** с поворотом, **произвольная** без поворота - маршрутная перестановка

Лекция 5:

- **Шифр Виженера**

Шифр Виженера

A	T	T	A	C	K	T	O	N	I	G	H	T
D	A	R	K	D	A	R	K	D	A	R	K	D

Текст:
 «Attack tonight»

Ключевое слово:
 «Dark»

Шифртекст:
 «DTKKFKKYQIXRW»

- **Шифр Бэкона** - двухбуквенный шифр, есть 2 режима:
 1. Алфавитный метод
 2. Циклические последовательности
- **Великий шифр** - каждое число замещало французский слог
- **Шифр Гронсфельда**

Шифр Гронсфельда

	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	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

V	I	C	T	O	R	Y
2	0	1	6	2	0	1

Текст: «Victory»

Ключ: K=2016

Длина текст = 9 ->

Ключ K=2016201

Шифртекст:

«XIDZQRZ»

- **Шифр Плейфера** - шифр простой замены биграмм

Шифр Плейфера (Уитстона)

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

Сообщение: «Hide the gold in the tree stump»

HI DE TH EG OL DI NT HE TR EX ES TU MP

BM ND ZB XD KY BE JV DM UI XM MN UV IF

- **Два квадрата**

Лекция 6:

- **Шифратор Джефферсона** - 36 дисков, 26 букв на каждом
- **Простая литорея** - Выписывались в строку подряд все согласные в количестве 10 букв. Под этой строкой составлялась вторая строка из последующих 10 согласных, записанных в обратном порядке. Гласные, Й, Ъ, Ь не заменялись
- **Мудрая литорея** - заменяются все буквы - простая замена
- **Хвиоть**

«Хвиоть» («фиоть»)

- Система основана на использовании букв, имеющих известное числовое значение. Такие буквы-числа для тайнописи раскладывались на слагаемые (обычно на два слагаемых).

$$\begin{aligned} \Delta &= 4 = 2 + 2 = \text{ВВ} \\ \text{Е} &= 5 = 3 + 2 = \text{ГВ} \\ \text{О} &= 70 = 50 + 20 = \text{НК} \end{aligned}$$

Δ	к	Г	Δ	е	5	з
лз	вбд	квгбдль	добро	ость	вело	зоялй
1	2	3	4	5	6	7
и	ю	1	к	л	м	н
инб	фитб	и	кнбо	лбди	мыслбте	наш
8	9	10	20	30	40	50
ж	о	п	ч	р	с	т
ж	о	п	ч	р	с	т
нов	он	покой	черь	рцз	слово	твердо
60	70	80	90	100	200	300
у	ф	х	ц	ш	щ	
ук	ферг	ха	пси	от	цы	
400	500	600	700	800	900	

Буквенные обозначения цифр и чисел

- Шифр А.Г.Головкина** - пропорциональная замена - согласной по одному шифробозначени, гласной - по два, 13 пустышек, обозначение для точек и запятых
- Биграммный шифр**
- Биклавный шифр**
- Шифр вертикальной перестановки** - маршрутная перестановка

Б	О	Ж	Е	Ц	А	Р	Я	Х	Р	А	Н	И
3	8	5	4	12	1	9	13	11	10	2	7	6
С	О	О	Б	Щ	И	Т	Е	О	П	Р	И	Б
Ы	Т	И	И	Л	И	Н	Е	Й	Н	Ы	Х	К
О	Р	А	Б	Л	Е	Й						

ИИЕ РЫ СЫО БИБ ОИА БК ИХ ОТР
ТНЙ ПН ОЙ ЩЛЛ ЕЕ

Лекция 7:

- “Массонский шифр”** - простая замена
- Шифр “Рельсовый забор”** - маршрутная перестановка
- Шифр Джефферсона Дэвиса** - division → 265-2-10 265 страница, 2 колонка и 10 слово - книжный шифр
- Шифр Стейджера** - маршрутная перестановка

- *Шифр для передачи флажками*

Лекция 8:

- *Шифры Биля* - книжный шифр
- *Цилиндр Базери* - 20 дисков, порядок букв не был секретным и образовывался из фраз-лозунгов
- *Пляшущие человечки* -простая замена
- *Долина страха* - книжный шифр