Шифры

Лекция 1:

- *Сциталь* - 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

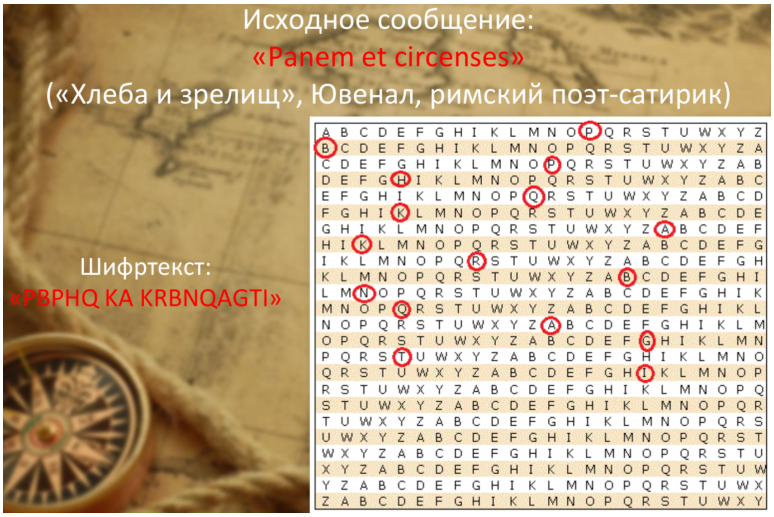
Лекция 3:

- *Колонная перестановка* - запись в таблицу и чтение по колонкам сверху вниз слева направо - маршрутная перестановка
- *Обратный порядок записи*
- *Редукция гласных*
- *Магические квадраты* - размера n*n, буквы открытого текста записываются в квадрат в соответсвии с нумерацией его клеток - муршрутная 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 “A” на внешнем. Первая буква сообщения ищется на внешнем диске и заменяется на букву внутреннего диска, далле сдвиг на 1 и тд
- *Диск Альберти режим 3* - индикаторная буква устанавливается напротив буквы “A”. Первая буква сообщения ищется на внешнем диске и заменяется на букву внутреннего диска, далле сдвиг на 1 и тд
- *Диск Альберти режим 4* - произвольная буква устанавливается напротив буквы “A” и записывается в виде заглавной, несколько символов шифруются без сдвига внутреннего диска. Далее в шифртексте снова ставится заглавная буква напротив буквы “A” , задающая новое положение диска и тд
- *Диск Альберти режим 5* - выбирается пароль, первая буква пароля совмещается с буквой “A” внешнего текста, шифруется первая буква открытого текста. Далее с буквой “A” совмещается вторая буква пароля и шифруется вторая буква текста и тд

Лекция 4:

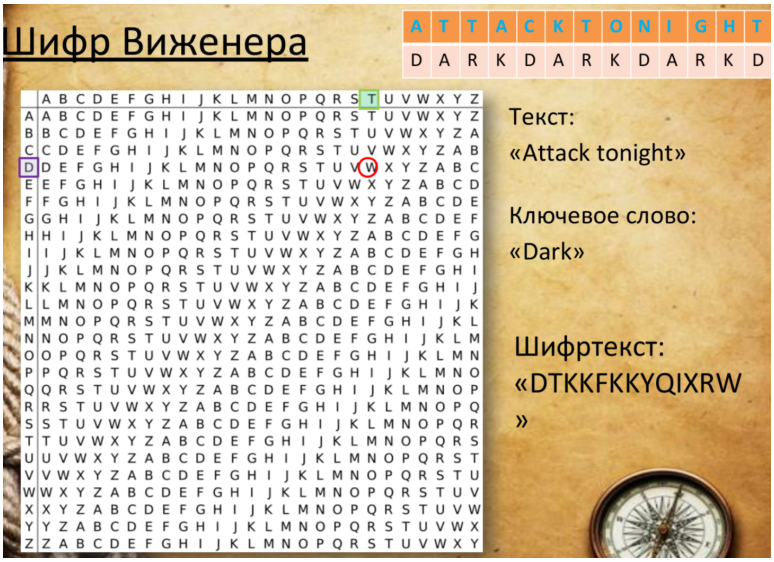
- *Миланский ключ* - гласным буквам ставилось в соответсвие несколько знаков шифруемого алфавита, число которых пропорционально частоте встречаемости буквы в открытом тексте
- *Омофонная замена* - не является многоалфавитным шифром
- *Шифр Марии Стюарт*
- *Таблица Тритемия* - многоалфавитный шифр - состоит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



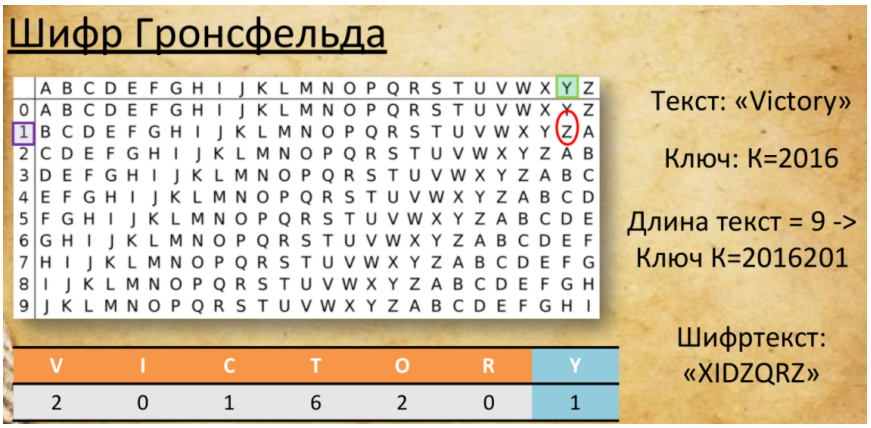
- *Решётка Кардано* - ***квадратная*** с поворотом, ***произвольная*** без поворота - маршрутная перестановка

Лекция 5:

- *Шифр Виженера*



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



- *Шифр Плейфера* - шифр простой замены биграмм

- *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*

- *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 секретныи и образовывался из фраз-лозунгов
- *Пляюшущие человечки* -простая замена
- *Долина страха* - книжный шифр