# Защита информации Лекция 3 (21.09.2022)

Уязвимость — это свойство системы допускающая или реализующая создание угроз.

### Шифрование

Шифрование – это преобразование открытого текста в зашифрованный текст с целью защитить его конфиденциальности.

Encryption  
plain text  
cipher text  
enciphering  
deciphering

### Принципы и требования Кирхгоффа

* Массовость
* Эмпирическая проверка

### Требования:

* Сложность расшифровки и модификации исходного сообщения
* Малые изменения исходного текста, влекут значительные изменения зашифрованного текста
* Область определения ключа должна исключать его перебор
* Стоимость дешифрации значительно превышает стоимость данных

Алгоритмы шифрование бывают симметричные и ассиметричные.

Симметричные – для шифрования и дешифрования используют один и тот же ключ.

* перестановки (permutations) P-преобразования;
* замены (substitution) S-преобразования;

### [Метод Скитала](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D0%B8%D1%82%D0%B0%D0%BB%D0%B0)



### Перестановка по правилу

Текст –> сеТк

42134

### Шифр Цезаря

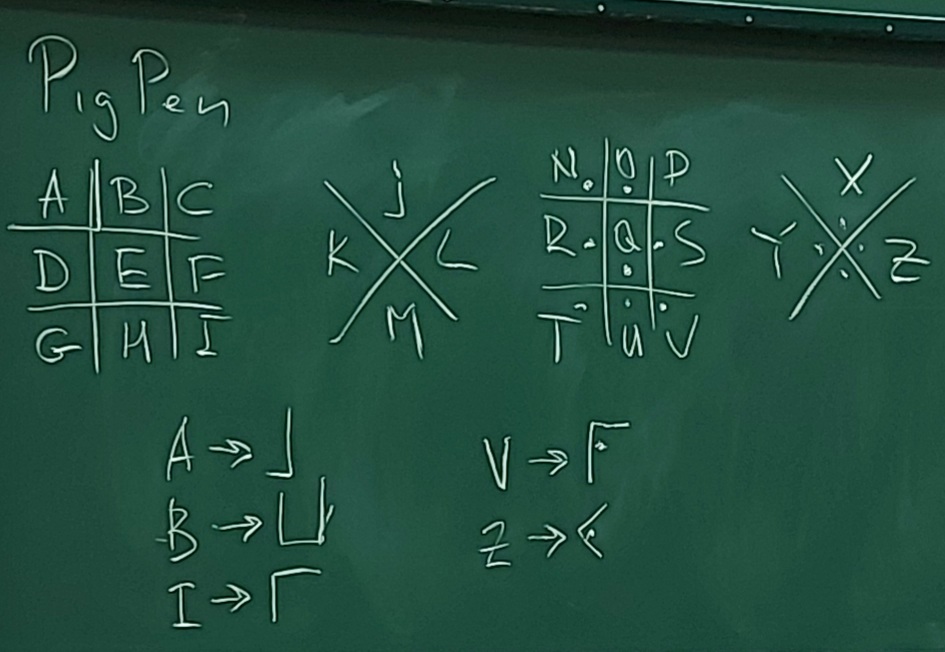
Сдвиг алфавита на 3

### [Квадрат Полибия](https://ru.wikipedia.org/wiki/%D0%9A%D0%B2%D0%B0%D0%B4%D1%80%D0%B0%D1%82_%D0%9F%D0%BE%D0%BB%D0%B8%D0%B1%D0%B8%D1%8F#%D0%A1%D0%BF%D0%BE%D1%81%D0%BE%D0%B1_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F)

|  |  |  |  |
| --- | --- | --- | --- |
| A | B | C | D |
| E | F | G | H |
|  |  |  |  |
|  |  |  |  |

A–>E

### [PigPen](https://ru.wikipedia.org/wiki/Pigpen)

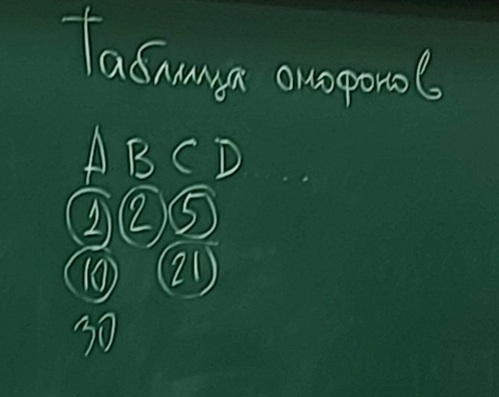


Все это одно алфавитные алгоритмы

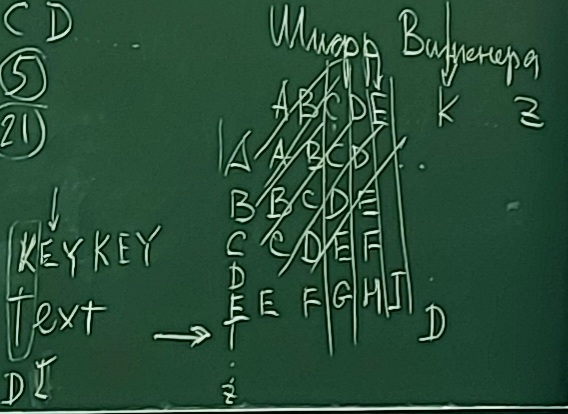
Многоалфавитные алгоритмы шифруют разные символы разными алфавитами.

### Таблица омофонов

A B C D …



### [Шифр Виженера](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B0)



### [Великий шифр Людовика 14ого](https://translated.turbopages.org/proxy_u/en-ru.ru.9abeb797-632b430b-673e6742-74722d776562/https/en.wikipedia.org/wiki/Great_Cipher)

### Поточные алгоритмы

Используют еще и предыдущие данные

### [Enigma](https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D0%B8%D0%B3%D0%BC%D0%B0)

2ая лаба – написать шифр энигмы для файла – 256 бит