Оглавление

[Введение 2](#_Toc207817315)

[Факторы, определяющие рост спроса на ИМ 3](#_Toc207817316)

Введение

64 часов лекций и практик

Оценивание:

* 30(Кт1) + 30(Кт2) + 40(ДЗ + посещаемость)

Контрольные точки — это проектно-аналитические работы.

Компьютерная Криптография

Криптография - наука о методах преобразования информации с целью ее защиты от несанкционированного доступа

* ﻿﻿Открытый текст (**plaintext** или **cleartext**)
* ﻿﻿Шифрование (**encryption**) - изменение исходного текста для того, чтобы скрыть его содержание
* ﻿﻿Шифротекст (**ciphertext**) - зашифрованное сообщение
* ﻿﻿Дешифрование (**decryption**)
* Ключ (**кеу**) шифрования

Этапы развития:

* ﻿Наивная (до начала XVI в.)
* ﻿﻿Формальная (XVI в. - начало ХХ в.)
* ﻿﻿Научная (30-60 годы XX в.)
* ﻿﻿Компьютерная (с 60 г. ХХ в.)

Шифр цезаря (отставание на 3):

ABCDEFGHIJKI.MNOPORSTUVWXYZ

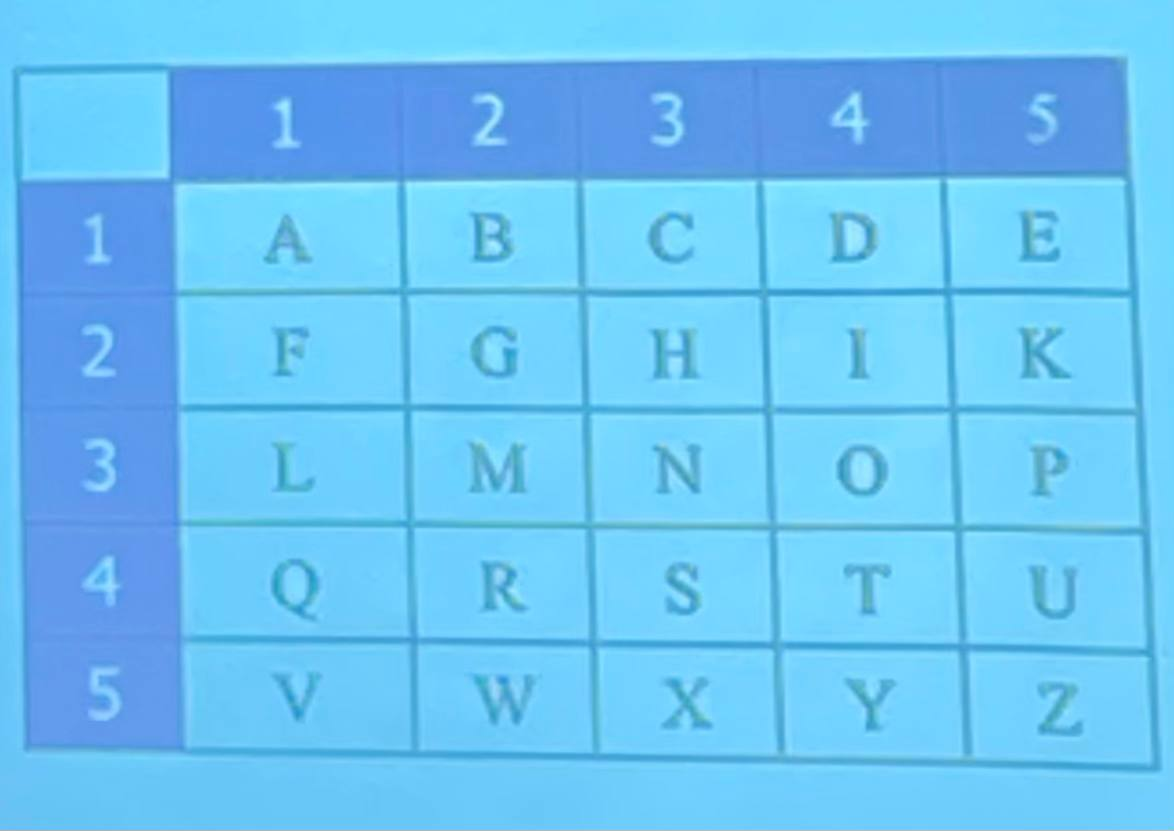
DEFGHIJKLMNOPORSTUVWXYZABC

VENI VIDI VICI

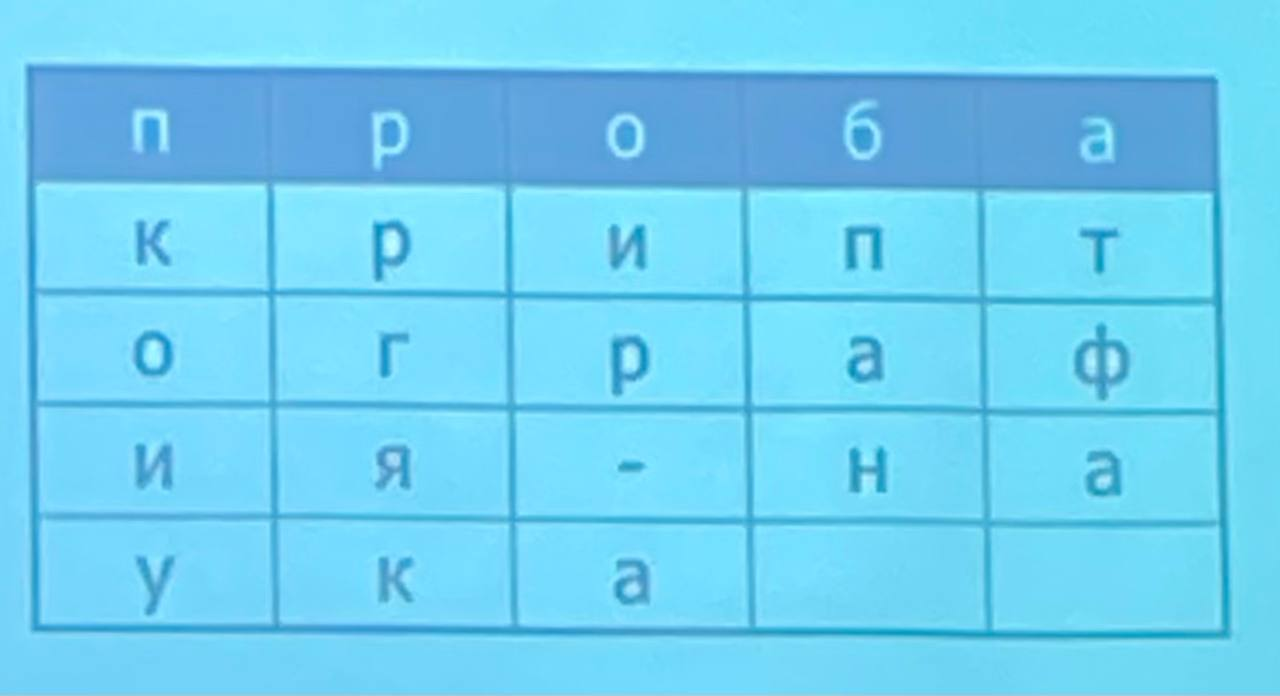
YHQL Y….

ДЗ реализовать

Шифр Полибия:



Шифр перестановки (табличная самая простая):



ДЗ – шифр цезаря и табличная перестановка.