# ТЕМА 3. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

## Применение алгоритмов шифрования. Шифры перестановки

# Практическое занятие 3/3
# Шифры перестановки

## Учебные вопросы:

1. Блочное шифрование
2. Шифрующие таблицы

# Вопрос 1. Блочное шифрование

Одним из первых физических приборов, реализующих шифр перестановки, является так называемый прибор «**Сцитала**». Он был изобретён в древней «варварской» Спарте во времена Ликурга (**V в. до н. э**.). Рим быстро воспользовался этим прибором.

# Блочное шифрование

Для шифрования текста использовался цилиндр заранее обусловленного диаметра. На цилиндр наматывался тонкий ремень из пергамента, и текст выписывался построчно по образующей цилиндра (вдоль его оси). Затем ремень сматывался и отправлялся получателю сообщения.

# Блочное шифрование

Последний наматывал его на цилиндр того же диаметра и читал текст по оси цилиндра.

В этом примере **ключом** шифра являлся диаметр цилиндра и его длина. Шифр «Сцитала» реализует один из вариантов так называемого ***«шифра маршрутной перестановки».***

# Блочное шифрование

Изобретение дешифровального устройства — «**Антисцитала**» — приписывается великому **Аристотелю**. Он предложил использовать конусообразное «копье», на которое наматывался перехваченный ремень; этот ремень передвигался по оси до того положения, пока не появлялся осмысленный текст.

# Блочное шифрование

## «Магический квадрат»

В квадрат размером 4x4 (размеры могли быть и другими) вписывались числа от 1 до 16.

Его магия состояла в том, что сумма чисел по строкам, столбцам и полным диагоналям равнялась одному и тому же числу — 34.

# Блочное шифрование

| | | | |
|---|---|---|---|
| 6 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

**УИРДЗЕПОСЖАОЕЯНП**

# Блочное шифрование

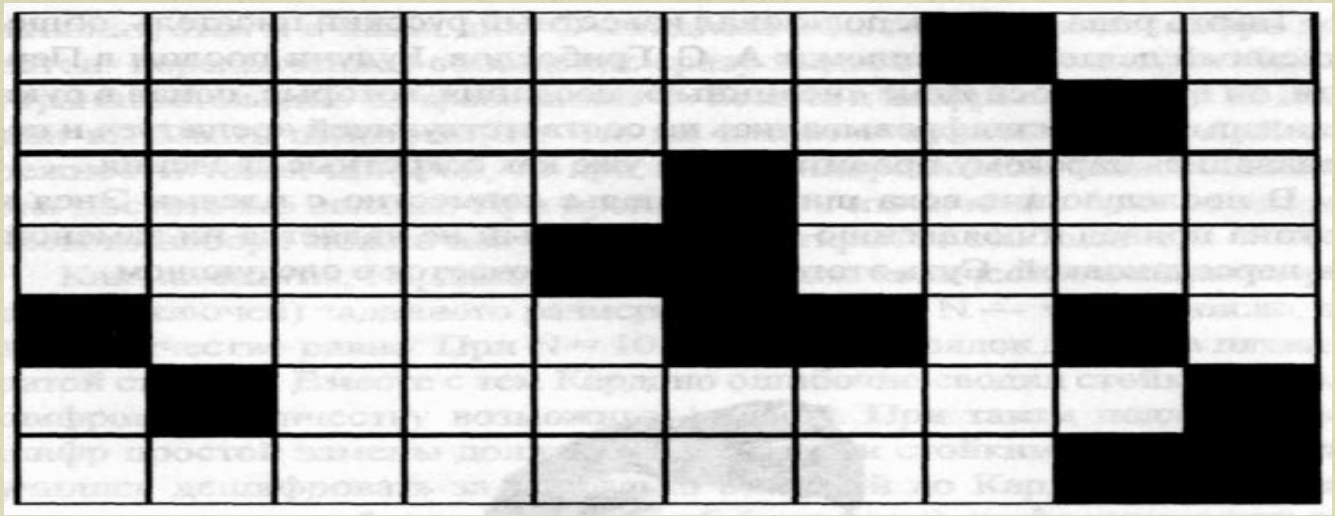
| | | | |
|---|---|---|---|
| 6(У) | 3(И) | 2(Р) | 13(Д) |
| 5(З) | 10(Е) | 11(Г) | 8(ю) |
| 9(С) | 6(Ж) | 7(А) | 12(О) |
| 4(Е) | 15(Я) | 14(Н) | 1(П) |

# Блочное шифрование

Примерно в **1550** г появилась книга математика, врача и философа Дж. **Кордано** в которой имелись разделы, посвященные криптографии.

Предложенный Кордано ***«шифр-решетка»*** лежит в основе знаменитого «шифра **Ришелье**», в котором шифрованный текст внешне имел вид «невинного» послания.

# Блочное шифрование



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | в | | |
| | | | | | | | | с | |
| | | | | | т | | | | |
| | | | | р | е | | | | |
| ч | | | | | а | з | | а | |
| | в | | | | | | | | т |
| | | | | | | | | р | а |

# Блочное шифрование

1. МТАЕКЛАОРТОСВИАП

2. АКГЯИЕОТЯ
   НТРИНЗЯБ.С

3. БИУРДПЕРТОВТОАВНРИЕММРЯЕТ

# Блочное шифрование

Выберем целое положительное число, скажем, 5; расположим числа от 1 до 5 в двухстрочной записи, в которой вторая строка — произвольная перестановка чисел верхней строки

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 3 | 2 | 5 | 1 | 4 |

# Блочное шифрование

Зашифруем фразу

**«РИМСКАЯ ИМПЕРИЯ»**

**РИМСК А ЯИМП ЕРИЯ**

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 3 | 2 | 5 | 1 | 4 |

# Блочное шифрование

| р | и | м | с | к | а | я | и | м | п | е | р | и | я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 |

| 3 | 2 | 5 | 1 | 4 | 3 | 2 | 5 | 1 | 4 | 3 | 2 | 5 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| м | и | к | р | с | и | я | п | а | м | и | р | я | е |

# Блочное шифрование

- РХООЯШПАООДГА (ключ=4Х3142)
- ДМФОИАИИКЦНЯОИФАРИМЦИ (ключ=5х31524)
- ЬОТКПЮМЕРЗЕЫВНИОИЛЩКМ (ключ=7х5271463)

# Вопрос 2. Шифрующие таблицы

Зашифруем слово **КУРСАНТ**

| 1 | 2 | 3 |
|---|---|---|
| К | С | Т |
| У | А | |
| Р | Н | |

| 2 | 3 | 1 |
|---|---|---|
| С | Т | К |
| А | | У |
| Н | | Р |

**КСТУАРН** **СТКАУНР**

# Шифрующие таблицы

Зашифруем слово

**КРИМИНАЛИСТИКА**

| 1 | 2 | 3 |
|---|---|---|
| К | М | А |
| Р | И | Л |
| И | Н | И |

| 1 | 2 | 3 |
|---|---|---|
| С | К | |
| Т | А | |
| И | | |

**КМАРИЛННИСКТАИ**

# Шифрующие таблицы

**Расшифруем: КМИИАОФЯЦДИ**

**(ключ = 3Х5Х31524)**

**Для этого посчитаем количество букв = 11**

| 3 | 1 | 5 | 2 | 4 |
|---|---|---|---|---|
| К | М | | И | И |
| А | О | | Ф | Я |
| Ц | Д | | И | |

# Шифрующие таблицы

**Расшифровать:**

- **АПЖЗРААИНДЧИЕИЯРН (ключ = 6х5х52413)**
- **АЕАЦСТИТТИЛЯИИПЦО (ключ = 3х3х321)**