Овчинников Павел,
368606, 1.3, R3241

# Лабораторная работа №1

## Список заданий



## Задание №1

Возьму русский алфавит, добавлю в него пробел и уберу 3 буквы Ъ, Ы, Ь, чтобы общее количество символов в алфавите стало простым числом — это упростит вычисления. Так получаем следующий набор из $\mathrm{n} = 31$ символа, пронумерованный от $0$ до $\mathrm{n} - 1$:

| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Э | Ю | Я | □ [пробел] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Сообщение, которое я буду зашифровывать — «**ЛИНАЛ□КРУТОЙ**». И теперь обозначим матрицы-ключи:

$$\mathrm{A} = \begin{bmatrix} 7 & 29 \\ 5 & 11 \end{bmatrix}$$

$$det\ A = 7 \cdot 11 - 5 \cdot 29 = 77 - 145 = -68$$

$$\mathrm{B} = \begin{bmatrix} 2 & 1 & 3 \\ 8 & 6 & 4 \\ 9 & 15 & 27 \end{bmatrix}$$

$$det\ B = 2 \cdot 6 \cdot 27 + 9 \cdot 4 + 8 \cdot 3 \cdot 15 - 9 \cdot 6 \cdot 3 - \\ -27 \cdot 8 - 15 \cdot 4 \cdot 2 = 324 + 36 + 360 - 162 - \\ -216 - 120 = 720 - 498 = 222$$

$$\mathrm{C} = \begin{bmatrix} 4 & 3 & 1 & 6 \\ 7 & 20 & 9 & 12 \\ 14 & 8 & 5 & 28 \\ 16 & 2 & 15 & 19 \end{bmatrix}$$

$$det\ C = 4 \cdot (-6044) - 3 \cdot 923 + 3112 - 6 \cdot \\ \cdot (-2730) = -7453$$

Определитель каждой из матриц-ключей не равен нулю и не имеет общих делителей с $n$, т. к. $n$ — простое число.

Пришло время шифровать наше сообщение при помощи матриц-ключей и метода Хилла. Для этого представим сообщение как набор чисел по таблице преобразования выше и получим: $M = [12 \quad 9 \quad 14 \quad 0 \quad 12 \quad 30 \quad 11 \quad 17 \quad 20 \quad 19 \quad 15 \quad 10]$. Для разных матриц-ключей понадобится разное представление этого набора чисел (вектора), чтобы произведение было возможным и дало матрицу той же размерности.

$$\mathrm{M_A} = \mathrm{AM}\ (mod\ 31) = \begin{bmatrix} 7 & 29 \\ 5 & 11 \end{bmatrix} \begin{bmatrix} 12 & 14 & 12 & 11 & 20 & 15 \\ 9 & 0 & 30 & 17 & 19 & 10 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 345 & 98 & 954 & 570 & 691 & 395 \\ 159 & 70 & 390 & 242 & 309 & 185 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 4 & 5 & 24 & 12 & 9 & 23 \\ 4 & 8 & 18 & 25 & 30 & 30 \end{bmatrix}$$

Зашифрованное матрицей-ключом 2×2 сообщение выглядит так: **ДЕЧЛИЦДЗСШ□□**.

$$M_B = \mathrm{BM}\ (mod\ 31) = \begin{bmatrix} 2 & 1 & 3 \\ 8 & 6 & 4 \\ 9 & 15 & 27 \end{bmatrix} \begin{bmatrix} 12 & 9 & 14 & 0 \\ 12 & 30 & 11 & 17 \\ 20 & 19 & 15 & 10 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 96 & 105 & 84 & 47 \\ 248 & 328 & 238 & 142 \\ 828 & 1044 & 696 & 525 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 3 & 12 & 22 & 16 \\ 0 & 18 & 21 & 18 \\ 22 & 21 & 14 & 29 \end{bmatrix}$$

Зашифрованное матрицей-ключом 3×3 сообщение выглядит так: **ГЛХПАСФСХФНЯ**.

$$M_C = CM\ (mod\ 31) = \begin{bmatrix} 4 & 3 & 1 & 6 \\ 7 & 20 & 9 & 12 \\ 14 & 8 & 5 & 28 \\ 16 & 2 & 15 & 19 \end{bmatrix} \begin{bmatrix} 12 & 9 & 14 & 0 \\ 12 & 30 & 11 & 17 \\ 20 & 19 & 15 & 10 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 173 & 179 & 226 \\ 411 & 636 & 998 \\ 755 & 727 & 816 \\ 718 & 708 & 774 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 18 & 24 & 9 \\ 8 & 16 & 6 \\ 11 & 14 & 10 \\ 5 & 26 & 30 \end{bmatrix}$$

Зашифрованное матрицей-ключом 4×4 сообщение выглядит так: **СЧИЗПЁКНЙЕЩ□**.

Сымитирую вредоносное вмешательство, заменив три символа в каждом из зашифрованных сообщений на другие:

– Для сообщения **ДЕЧЛИЦДЗСШ□□** → **ДЕЧЛБЦДЗСШАЯ** → $M_A = \begin{bmatrix} 4 & 5 & 24 & 12 & 1 & 23 \\ 4 & 8 & 18 & 25 & 0 & 29 \end{bmatrix}$.

– Для сообщения **ГЛХПАСФСХФНЯ** → **ДЛХПРСФСРФНЯ** → $M_B = \begin{bmatrix} 4 & 12 & 22 & 16 \\ 17 & 18 & 21 & 18 \\ 17 & 21 & 14 & 29 \end{bmatrix}$.

– Для сообщения **СЧИЗПЁКНЙЕЩ□** → **СЧИЗПЁКНЙАБВ** → $M_C = \begin{bmatrix} 18 & 24 & 9 \\ 8 & 16 & 6 \\ 11 & 14 & 10 \\ 0 & 1 & 2 \end{bmatrix}$.

Теперь расшифруем взломанные сообщения, но для начала нужно найти обратные матрицы:

$$A^{-1}\ (mod\ 31) = (\det \mathrm{A})^{-1} \begin{bmatrix} C_{11} & C_{21} \\ C_{12} & C_{22} \end{bmatrix} (mod\ 31) = 5 \begin{bmatrix} 11 & -29 \\ -5 & 7 \end{bmatrix} (mod\ 31) = 5 \begin{bmatrix} 11 & -29 \\ -5 & 7 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 55 & -145 \\ -25 & 35 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 24 & 10 \\ 6 & 4 \end{bmatrix}$$

$$B^{-1}\ (mod\ 31) = (det\ B)^{-1} \begin{bmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{bmatrix} (mod\ 31) = 25 \begin{bmatrix} 102 & 18 & -14 \\ -180 & 27 & 16 \\ 66 & -21 & 4 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 8 & 16 & 22 \\ 26 & 24 & 28 \\ 7 & 2 & 7 \end{bmatrix}$$

$$C^{-1}\ (mod\ 31) = (det\ C)^{-1} \begin{bmatrix} C_{11} & C_{21} & C_{31} & C_{41} \\ C_{12} & C_{22} & C_{32} & C_{42} \\ C_{13} & C_{23} & C_{33} & C_{43} \\ C_{14} & C_{24} & C_{34} & C_{44} \end{bmatrix} (mod\ 31) = 19 \begin{bmatrix} -6044 & 411 & 1309 & -280 \\ -923 & -338 & 211 & 194 \\ 3112 & -330 & -235 & -428 \\ 2730 & -50 & -939 & 161 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 19 & 28 & 9 & 12 \\ 9 & 26 & 10 & 28 \\ 11 & 23 & 30 & 21 \\ 7 & 11 & 15 & 21 \end{bmatrix}$$

И, наконец, займёмся расшифровкой, домножив слева матрицы сообщений на матрицы выше:

$$\mathrm{A^{-1}M_A}\ (\mathrm{mod}\ 31) = \begin{bmatrix} 24 & 10 \\ 6 & 4 \end{bmatrix} \begin{bmatrix} 4 & 5 & 24 & 12 & 1 & 23 \\ 4 & 8 & 18 & 25 & 0 & 29 \end{bmatrix} (\mathrm{mod}\ 31) = \begin{bmatrix} 136 & 200 & 756 & 538 & 24 & 842 \\ 40 & 62 & 216 & 172 & 6 & 254 \end{bmatrix} (\mathrm{mod}\ 31) = \begin{bmatrix} 12 & 14 & 12 & 11 & 24 & 5 \\ 9 & 0 & 30 & 17 & 6 & 6 \end{bmatrix}$$

Расшифрованное обратной матрице-ключу матрицей 2×2 сообщение выглядит так: **ЛНЛКЧЕИА□РЁЁ**.

$$B^{-1}M_B\ (mod\ 31) = \begin{bmatrix} 8 & 16 & 22 \\ 26 & 24 & 28 \\ 7 & 2 & 7 \end{bmatrix} \begin{bmatrix} 4 & 12 & 22 & 16 \\ 17 & 18 & 21 & 18 \\ 17 & 21 & 14 & 29 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 678 & 846 & 820 & 1054 \\ 988 & 1332 & 1468 & 1660 \\ 181 & 267 & 294 & 351 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 27 & 9 & 14 & 0 \\ 27 & 30 & 11 & 17 \\ 26 & 19 & 15 & 10 \end{bmatrix}$$

Расшифрованное обратной матрице-ключу матрицей 3×3 сообщение выглядит так: **ЭИНАЭ□КРЩТОЙ**.

$$C^{-1}M_C \ (mod\ 31) = \begin{bmatrix} 19 & 28 & 9 & 12 \\ 9 & 26 & 10 & 28 \\ 11 & 23 & 30 & 21 \\ 7 & 11 & 15 & 21 \end{bmatrix} \begin{bmatrix} 18 & 24 & 9 \\ 8 & 16 & 6 \\ 11 & 14 & 10 \\ 0 & 1 & 2 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 665 & 1042 & 453 \\ 480 & 800 & 393 \\ 712 & 1073 & 579 \\ 379 & 575 & 321 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 14 & 19 & 19 \\ 15 & 25 & 21 \\ 30 & 19 & 21 \\ 7 & 17 & 11 \end{bmatrix}$$

Расшифрованное обратной матрице-ключу матрицей 4×4 сообщение выглядит так: **НТТОШФ□ТФЖРК**.

**Вывод**: при замене хотя бы одной из букв в зашифрованном сообщении теряется всё исходное сообщение, так как во время матричного умножения буквы связываются между собой. В криптографии это называется «лавинным эффектом» или диффузией по Шеннону, когда избыточность данных «распределяется» по всей структуре выходных данных. Всё же при изменении зашифрованного сообщения в некоторых случаях, как видно с матрицей-ключом 3×3, распознать исходное сообщение можно, но чаще всего оно полностью видоизменяется.

## Задание №2

Продублирую ниже алфавит, который мы будем использовать в этом задании:

| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Э | Ю | Я | □ [пробел] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Программу, генерирующую матрицу-ключ 2×2 и шифрующую с помощью этого ключа сообщения из 12 символов, предоставляю **здесь** ←

Первое сообщение остаётся таким же — **ЛИНАЛ□КРУТОЙ**. Второе сообщение будет таким — **ХЭЛОУ□ЕЖИДЗЕ**. Зашифруем их с помощью ключа, который программа не предоставляет до тех пор, пока я не попрошу.

```
Enter command: encrypt ЛИНАЛ КРУТОЙ
Original matrix:
12      9       14      0       12      30
11      17      20      19      15      10

Encrypted matrix:
4       6       21      26      16      4
20      4       22      8       7       10
```

```
Enter command: encrypt ХЭЛОУ ЕЖИДЗЕ
Original matrix:
22      27      12      15      20      30
5       7       9       4       8       5

Encrypted matrix:
29      10      29      30      17      20
2       0       11      16      23      3
```

Ведущим сообщением и в этот раз будет **ЛИНАЛ□КРУТОЙ**. С ним и будем проводить манипуляции, чтобы восстановить второе исходное сообщение, имея только его зашифрованный вариант. Так как ключ для шифрования всего сообщения одинаковый, мы можем отбросить все символы, кроме первых четырёх. Поэтому рассмотрим операцию $\mathrm{KM} = \mathrm{M_K}$, где $M$ — матрица из первых четырёх чисел исходного сообщения, а $M_K$ — матрица из первых четырёх чисел зашифрованного сообщения:

$$\mathrm{KM} = M_K \Leftrightarrow \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \begin{bmatrix} 12 & 9 & 14 & 0 & 12 & 30 \\ 11 & 17 & 20 & 19 & 15 & 10 \end{bmatrix} = \begin{bmatrix} 4 & 6 & 21 & 26 & 16 & 4 \\ 20 & 4 & 22 & 8 & 7 & 10 \end{bmatrix}$$

$$\begin{bmatrix} 12x_1 + 11x_2 & 9x_1 + 17x_2 & 14x_1 + 20x_2 & 19x_2 & 12x_1 + 15x_2 & 30x_1 + 10x_2 \\ 12x_3 + 11x_4 & 9x_3 + 17x_4 & 14x_3 + 20x_4 & 19x_4 & 12x_3 + 15x_4 & 30x_3 + 10x_4 \end{bmatrix} = \begin{bmatrix} 4 & 6 & 21 & 26 & 16 & 4 \\ 20 & 4 & 22 & 8 & 7 & 10 \end{bmatrix}$$

Получаем систему уравнений, которую можно решить, используя небольшую программу. Проверим, совпадает ли найденные значения с матрицей-ключом, которая хранится в программе:

```python
for i in range(33):
    for j in range(33):
        if ((12 * i + 11 * j) % 31 == 4 and (9 * i + 17 * j) % 31 == 6 and (14 * i + 20 * j) % 31 == 21
                and (19 * j) % 31 == 26 and (12 * i + 15 * j) % 31 == 16 and (30 * i + 10 * j) % 31 == 4):
            print(i, j)  # >>> 26 3

for i in range(33):
    for j in range(33):
        if ((12 * i + 11 * j) % 31 == 20 and (9 * i + 17 * j) % 31 == 4 and (14 * i + 20 * j) % 31 == 22
                and (19 * j) % 31 == 8 and (12 * i + 15 * j) % 31 == 7 and (30 * i + 10 * j) % 31 == 10):
            print(i, j)  # >>> 4 20
```

```
Enter command: show key
26      3
4       20
```

Проверить работу кода можно **здесь** ←

Найдём от матрицы-ключа обратную:

$$K^{-1} \ (mod\ 31) = (det\ A)^{-1} \begin{bmatrix} 20 & -3 \\ -4 & 26 \end{bmatrix} (mod\ 31) = 13 \begin{bmatrix} 20 & -3 \\ -4 & 26 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 260 & -39 \\ -52 & 338 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 12 & 23 \\ 10 & 28 \end{bmatrix}$$

Теперь выполним произведение обратного ключа на зашифрованную матрицу, чтобы получить исходный текст:

$$\begin{bmatrix} 12 & 23 \\ 10 & 28 \end{bmatrix} \begin{bmatrix} 29 & 10 & 29 & 30 & 17 & 20 \\ 2 & 0 & 11 & 16 & 23 & 3 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 394 & 120 & 601 & 728 & 733 & 309 \\ 346 & 100 & 598 & 748 & 814 & 284 \end{bmatrix} (mod\ 31) = \begin{bmatrix} 22 & 27 & 12 & 15 & 20 & 30 \\ 5 & 7 & 9 & 4 & 8 & 5 \end{bmatrix}$$

Кажется, совпадает! Проверим побуквенно: 22 = Х, 27 = Э, 12 = Л, 15 = О, 20 = У, 30 = □, 5 = Е, 7 = Ж, 9 = И, 4 = Д, 8 = З, 5 = Е. И получаем исходную фразу **ХЭЛОУ□ЕЖИДЗЕ**.

**Вывод**: не имея на руках ключа, но имея оригинал и зашифрованное сообщение, можно выявить линейную зависимость шифра, получить матрицу-ключ и взломать шифр, чтобы в дальнейшем расшифровать любой зашифрованное сообщение.