

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего
образования

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИТМО

Факультет систем управления и робототехники

Лабораторная работа № 1
"Кодирование и шифрование"
по дисциплине Практическая линейная алгебра

Выполнила: студентка гр. **R3238**

Нечаева А. А.

Преподаватель: *Перегудин Алексей Алексеевич*

Санкт-Петербург, 2023-2024

1 Задание 1. Шифр Хилла

1.1 Задание алфавита и сообщения

Таблица 1 – Используемый алфавит

Символ	Код	Символ	Код	Символ	Код
А	0	З	4	Ы	8
В	1	Л	5	Ь	9
Д	2	Н	6	Я	10
Ё	3	П	7		

Зашифрованное сообщение: **ЗВЕЁЗДНАЯПЫЛЬ**

Размер алфавита в нашем случае:

$$n = 11$$

У числа **11** нет делителей, кроме единицы и самого числа.

1.2 Шифрование с помощью матрицы-ключа 2×2

Матрица-ключ размера 2×2 :

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \quad (1)$$

Проверка определителя:

$$\begin{vmatrix} 1 & 2 \\ 4 & 9 \end{vmatrix} = 1 \neq 0 \quad (2)$$

Запишем фразу, подлежащую шифрованию с помощью кодов символов алфавита и разобьем наше сообщение на векторы.

Далее представлены фрагменты сообщения и соответствующие векторы кодов:

$$\begin{aligned} \mathbf{ЗВ} &\rightarrow \begin{pmatrix} 4 \\ 1 \end{pmatrix}; \mathbf{ЁЗ} \rightarrow \begin{pmatrix} 3 \\ 4 \end{pmatrix}; \mathbf{ДН} \rightarrow \begin{pmatrix} 2 \\ 6 \end{pmatrix}; \mathbf{АЯ} \rightarrow \begin{pmatrix} 0 \\ 10 \end{pmatrix} \\ \mathbf{ПЫ} &\rightarrow \begin{pmatrix} 7 \\ 8 \end{pmatrix}; \mathbf{ЛЬ} \rightarrow \begin{pmatrix} 5 \\ 9 \end{pmatrix} \end{aligned}$$

Теперь зашифруем сообщение: матрично умножим ключ на каждый вектор и найдем остаток от деления на размер алфавита от результата:

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 4 \\ 1 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 25 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 3 \end{pmatrix} \quad (3)$$

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 3 \\ 4 \end{pmatrix} \pmod{11} = \begin{pmatrix} 11 \\ 48 \end{pmatrix} \pmod{11} = \begin{pmatrix} 0 \\ 4 \end{pmatrix} \quad (4)$$

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 2 \\ 6 \end{pmatrix} \pmod{11} = \begin{pmatrix} 14 \\ 62 \end{pmatrix} \pmod{11} = \begin{pmatrix} 3 \\ 7 \end{pmatrix} \quad (5)$$

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 0 \\ 10 \end{pmatrix} \pmod{11} = \begin{pmatrix} 20 \\ 90 \end{pmatrix} \pmod{11} = \begin{pmatrix} 9 \\ 2 \end{pmatrix} \quad (6)$$

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 7 \\ 8 \end{pmatrix} \pmod{11} = \begin{pmatrix} 23 \\ 100 \end{pmatrix} \pmod{11} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad (7)$$

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 5 \\ 9 \end{pmatrix} \pmod{11} = \begin{pmatrix} 23 \\ 101 \end{pmatrix} \pmod{11} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad (8)$$

Декодируем полученный результат:

$$\begin{pmatrix} 6 \\ 3 \end{pmatrix} \rightarrow \mathbf{HE} ; \begin{pmatrix} 0 \\ 4 \end{pmatrix} \rightarrow \mathbf{AZ} ; \begin{pmatrix} 3 \\ 7 \end{pmatrix} \rightarrow \mathbf{EP} ; \begin{pmatrix} 9 \\ 2 \end{pmatrix} \rightarrow \mathbf{BD} ;$$

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \rightarrow \mathbf{BV} ; \begin{pmatrix} 1 \\ 2 \end{pmatrix} \rightarrow \mathbf{VD}$$

Полученное сообщение: **HEAZEPBVDVVVD**

1.3 Шифрование с помощью матрицы-ключа 3×3

Матрица-ключ размера 3×3 :

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad (9)$$

Проверка определителя:

$$\begin{vmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{vmatrix} = 1 \neq 0 \quad (10)$$

Разобьем сообщение на фрагменты длины 3 и запишем соответствующие им векторы кодов:

$$\begin{aligned}
\mathbf{ЗВЁ} &\rightarrow \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix}; \\
\mathbf{ЗДН} &\rightarrow \begin{pmatrix} 4 \\ 2 \\ 6 \end{pmatrix}; \mathbf{АЯП} \rightarrow \begin{pmatrix} 0 \\ 10 \\ 7 \end{pmatrix}; \\
\mathbf{ЫЛЬ} &\rightarrow \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix}
\end{aligned}$$

Повторяем действия, описанные в разделе 1.2:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} \quad (11)$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 4 \\ 2 \\ 6 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 6 \\ 10 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 6 \\ 10 \end{pmatrix} \quad (12)$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 10 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 10 \\ 7 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 10 \\ 7 \\ 7 \end{pmatrix} \quad (13)$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix} \pmod{11} = \begin{pmatrix} 13 \\ 9 \\ 17 \end{pmatrix} \pmod{11} = \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix} \quad (14)$$

Декодируем:

$$\begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} \rightarrow \mathbf{ЛЁП}; \begin{pmatrix} 6 \\ 6 \\ 10 \end{pmatrix} \rightarrow \mathbf{ННЯ}; \begin{pmatrix} 10 \\ 7 \\ 7 \end{pmatrix} \rightarrow \mathbf{ЯПП}; \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix} \rightarrow \mathbf{ДЬН}$$

Полученное сообщение: **ЛЁПННЯЯППДЬН**

1.4 Шифрование с помощью матрицы-ключа 4×4

Матрица-ключ размера 4×4 :

$$C = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad (15)$$

Проверка определителя:

$$\begin{vmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{vmatrix} = -1 \neq 0 \quad (16)$$

Разобьем сообщение на фрагменты по 4 символа и представим векторы полученных кодов:

$$\begin{aligned} \mathbf{ЗВЁЗ} &\rightarrow \begin{pmatrix} 4 \\ 1 \\ 3 \\ 4 \end{pmatrix}; \\ \mathbf{ДНАЯ} &\rightarrow \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix}; \\ \mathbf{ПЫЛЬ} &\rightarrow \begin{pmatrix} 7 \\ 8 \\ 5 \\ 9 \end{pmatrix} \end{aligned}$$

Повторяем действия, описанные в разделе 1.2:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 4 \\ 1 \\ 3 \\ 4 \end{pmatrix} \pmod{11} = \begin{pmatrix} 9 \\ 3 \\ 11 \\ 5 \end{pmatrix} \pmod{11} = \begin{pmatrix} 9 \\ 3 \\ 0 \\ 5 \end{pmatrix} \quad (17)$$

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix} \pmod{11} = \begin{pmatrix} 18 \\ 0 \\ 12 \\ 8 \end{pmatrix} \pmod{11} = \begin{pmatrix} 7 \\ 0 \\ 1 \\ 8 \end{pmatrix} \quad (18)$$

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 7 \\ 8 \\ 5 \\ 9 \end{pmatrix} \pmod{11} = \begin{pmatrix} 24 \\ 5 \\ 21 \\ 15 \end{pmatrix} \pmod{11} = \begin{pmatrix} 2 \\ 5 \\ 10 \\ 4 \end{pmatrix} \quad (19)$$

Декодируем:

$$\begin{pmatrix} 9 \\ 3 \\ 0 \\ 5 \end{pmatrix} \rightarrow \text{БЁАЛ} ; \begin{pmatrix} 7 \\ 0 \\ 1 \\ 8 \end{pmatrix} \rightarrow \text{ПАВЫ} ; \begin{pmatrix} 2 \\ 5 \\ 10 \\ 4 \end{pmatrix} \rightarrow \text{ДЛЯЗ}$$

Полученное сообщение: **БЁАЛПАВЫДЛЯЗ**

1.5 Имитация вредоносного вмешательства

а) Повредим фразу, полученную в пункте 1.2

Таблица 2 – Повреждение первого результата

Исходные символы	Н	Ё	А	З	Ё	П	Б	Д	В	В	В	Д
После атаки	Н	Л	А	З	Б	П	Б	Д	Ы	В	В	Д
Коды после атаки	6	5	0	4	9	7	9	2	8	1	1	2

Найдем обратную матрицу от первого ключа:

$$A^{-1} = \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & -2 \\ -4 & 1 \end{pmatrix} \quad (20)$$

Разобьем фразу **НЛЯЗЬПДЫВВД** на фрагменты:

$$\begin{aligned} \text{НЛ} &\rightarrow \begin{pmatrix} 6 \\ 5 \end{pmatrix} ; \text{АЗ} \rightarrow \begin{pmatrix} 0 \\ 4 \end{pmatrix} ; \text{БП} \rightarrow \begin{pmatrix} 9 \\ 7 \end{pmatrix} ; \text{БД} \rightarrow \begin{pmatrix} 9 \\ 2 \end{pmatrix} ; \\ \text{ЫВ} &\rightarrow \begin{pmatrix} 8 \\ 1 \end{pmatrix} ; \text{ВД} \rightarrow \begin{pmatrix} 1 \\ 2 \end{pmatrix} \end{aligned}$$

Расшифруем сообщение:

$$\begin{pmatrix} 9 & -2 \\ -4 & 1 \end{pmatrix} \times \begin{pmatrix} 6 \\ 5 \end{pmatrix} \pmod{11} = \begin{pmatrix} 44 \\ -19 \end{pmatrix} \pmod{11} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \quad (21)$$

$$\begin{pmatrix} 9 & -2 \\ -4 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 4 \end{pmatrix} \pmod{11} = \begin{pmatrix} -8 \\ 4 \end{pmatrix} \pmod{11} = \begin{pmatrix} 3 \\ 4 \end{pmatrix} \quad (22)$$

$$\begin{pmatrix} 9 & -2 \\ -4 & 1 \end{pmatrix} \times \begin{pmatrix} 9 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 67 \\ -29 \end{pmatrix} \pmod{11} = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \quad (23)$$

$$\begin{pmatrix} 9 & -2 \\ -4 & 1 \end{pmatrix} \times \begin{pmatrix} 9 \\ 2 \end{pmatrix} \pmod{11} = \begin{pmatrix} 77 \\ -34 \end{pmatrix} \pmod{11} = \begin{pmatrix} 0 \\ 10 \end{pmatrix} \quad (24)$$

$$\begin{pmatrix} 9 & -2 \\ -4 & 1 \end{pmatrix} \times \begin{pmatrix} 8 \\ 1 \end{pmatrix} \pmod{11} = \begin{pmatrix} 70 \\ -31 \end{pmatrix} \pmod{11} = \begin{pmatrix} 4 \\ 2 \end{pmatrix} \quad (25)$$

$$\begin{pmatrix} 9 & -2 \\ -4 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ -2 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \quad (26)$$

Декодируем полученный результат:

$$\begin{pmatrix} 0 \\ 3 \end{pmatrix} \rightarrow \mathbf{АЁ} ; \begin{pmatrix} 3 \\ 4 \end{pmatrix} \rightarrow \mathbf{ЁЗ} ; \begin{pmatrix} 1 \\ 4 \end{pmatrix} \rightarrow \mathbf{ВЗ} ; \begin{pmatrix} 0 \\ 10 \end{pmatrix} \rightarrow \mathbf{АЯ} ;$$

$$\begin{pmatrix} 4 \\ 2 \end{pmatrix} \rightarrow \mathbf{ЗД} ; \begin{pmatrix} 5 \\ 9 \end{pmatrix} \rightarrow \mathbf{ЛЪ}$$

Полученное сообщение: **АЁ ЁЗ ВЗ АЯ ЗД ЛЪ**

Заметим, что поврежденными участками после расшифровки оказались те пары букв, в которых мы провели подмену символов.

б) Повредим фразу, полученную в пункте 1.3

Таблица 2 – Повреждение второго результата

Исходные символы	Л	Ё	П	Н	Н	Я	Я	П	П	Д	Ъ	Н
После атаки	Л	Ё	П	Н	Ы	А	Я	В	П	Д	Ъ	Н
Коды после атаки	5	3	7	6	8	0	10	1	7	2	9	6

Найдем обратную матрицу от второго ключа:

$$B^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & -1 \\ 0 & 1 & 0 \end{pmatrix} \quad (27)$$

Разобьем фразу **ЛЁПНЫАЯВПДЪН** на фрагменты:

$$\mathbf{ЛЁП} \rightarrow \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} ;$$

$$\mathbf{НЫА} \rightarrow \begin{pmatrix} 6 \\ 8 \\ 0 \end{pmatrix} ; \mathbf{ЯВП} \rightarrow \begin{pmatrix} 10 \\ 1 \\ 7 \end{pmatrix} ;$$

$$\mathbf{ДЪН} \rightarrow \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix}$$

Расшифруем сообщение:

$$\begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & -1 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \pmod{11} = \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \quad (28)$$

$$\begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & -1 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 6 \\ 8 \\ 0 \end{pmatrix} \pmod{11} = \begin{pmatrix} -8 \\ 14 \\ 8 \end{pmatrix} \pmod{11} = \begin{pmatrix} 3 \\ 3 \\ 8 \end{pmatrix} \quad (29)$$

$$\begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & -1 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 10 \\ 1 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 4 \\ 1 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 4 \\ 1 \end{pmatrix} \quad (30)$$

$$\begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & -1 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix} \pmod{11} = \begin{pmatrix} -3 \\ 5 \\ 9 \end{pmatrix} \pmod{11} = \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix} \quad (31)$$

Декодируем полученный результат:

$$\begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \rightarrow \text{ЗВЁ} ; \begin{pmatrix} 3 \\ 3 \\ 8 \end{pmatrix} \rightarrow \text{ЁЁЫ} ; \begin{pmatrix} 6 \\ 4 \\ 1 \end{pmatrix} \rightarrow \text{НЗВ} ; \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix} \rightarrow \text{ЫЛЬ}$$

Полученное сообщение: **ЗВЁ ЁЁЫ НЗВ ЫЛЬ**

Аналогично предыдущему пункту ошибки проявились только в тех фрагментах, в которых были заменены символы.

в) Повредим фразу, полученную в пункте 1.4

Таблица 3 – Повреждение третьего результата

Исходные символы	В	Л	П	П	Д	Д	Н	Д	Н	Я	З	Д
После атаки	В	Л	Ы	П	Ь	Д	Н	Д	Н	Я	З	А
Коды после атаки	1	5	8	7	9	2	6	2	6	10	4	0

Найдем обратную матрицу от третьего ключа:

$$\begin{pmatrix} 5 & 3 & 2 & 4 \\ 0 & 5 & 3 & 6 \\ 1 & 8 & 2 & 0 \\ 5 & 7 & 0 & 6 \end{pmatrix}^{-1} = \frac{1}{433} \begin{pmatrix} 84 & -58 & 3 & 2 \\ -39 & -4 & 45 & 30 \\ 114 & 45 & 35 & -121 \\ -\frac{49}{2} & 53 & -55 & \frac{71}{2} \end{pmatrix} \quad (32)$$

2 Задание 2. Взлом шифра Хилла

3 Задание 3. Код Хэмминга

4 Задание 4. Код Хэмминг?