

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:

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

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:

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

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:

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

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 **НЛЯЗЫПДЫВВД** на фрагменты:

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

Расшифруем сообщение:

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

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

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

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

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

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

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	Б	Ё	А	Л	П	А	В	Ы	Д	Л	Я	З
После атаки	В	П	А	Д	П	А	В	Ы	Д	Л	Я	З
Коды после атаки	1	7	0	2	7	0	1	8	2	5	10	4

Найдем обратную матрицу от третьего ключа:

$$C^{-1} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \quad (32)$$

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

$$\text{ВПАД} \rightarrow \begin{pmatrix} 1 \\ 7 \\ 0 \\ 2 \end{pmatrix} ;$$

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

Повторим привычные действия для расшифровки сообщения:

$$\begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 7 \\ 0 \\ 2 \end{pmatrix} (\text{mod } 11) = \begin{pmatrix} -6 \\ 8 \\ 7 \\ -1 \end{pmatrix} (\text{mod } 11) = \begin{pmatrix} 5 \\ 8 \\ 7 \\ 10 \end{pmatrix} \quad (33)$$

$$\begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \times \begin{pmatrix} 7 \\ 0 \\ 1 \\ 8 \end{pmatrix} (\text{mod } 11) = \begin{pmatrix} 2 \\ 6 \\ 0 \\ -1 \end{pmatrix} (\text{mod } 11) = \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix} \quad (34)$$

$$\begin{pmatrix} -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix} \times \begin{pmatrix} 2 \\ 5 \\ 10 \\ 4 \end{pmatrix} (\text{mod } 11) = \begin{pmatrix} 7 \\ -3 \\ 5 \\ -2 \end{pmatrix} (\text{mod } 11) = \begin{pmatrix} 7 \\ 8 \\ 6 \\ 9 \end{pmatrix} \quad (35)$$

Декодируем полученный результат:

$$\begin{pmatrix} 5 \\ 8 \\ 7 \\ 10 \end{pmatrix} \rightarrow \text{ЛЫПЯ} ; \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix} \rightarrow \text{ДНЯЯ} ; \begin{pmatrix} 7 \\ 8 \\ 6 \\ 9 \end{pmatrix} \rightarrow \text{ПЫЛЬ} ;$$

Полученное сообщение: **ЛЫПЯ ДНЯЯПЫЛЬ**

1.6 Вывод НУЖЕН ЛИ?

2 Задание 2. Взлом шифра Хилла

3 Задание 3. Код Хэмминга

Таблица 4 – Используемый алфавит

Символ	Код	Символ	Код	Символ	Код	Символ	Код
А	00000	И	01000	Р	10000	Ш	11000
Б	00001	Й	01001	С	10001	Щ	11001
В	00010	К	01010	Т	10010	Ъ	11010
Г	00011	Л	01011	У	10011	Ы	11011
Д	00100	М	01100	Ф	10100	Ь	11100
Е	00101	Н	01101	Х	10101	Э	11101
Ж	00110	О	01110	Ц	10110	Ю	11110
З	00111	П	01111	Ч	10111	Я	11111

Слово: **СОВА**. Соответствующий код: **10001 01110 00010 00000**.

3.1 Немного теории

G – порождающая матрица, размера 4×7 , по числу информационных и кодовых разрядов. Левая часть матрицы – участок 4×4 представляет собой единичную матрицу, а справа –

Кодирование производится по формуле:

$$Y = X \times G(\text{mod}2) \quad (36)$$

Получаем систематический код – код, в котором информационные разряды являются частью кодового вектора.

Для декодирования (проверки) используется проверочная матрица H размера 7×3 . Для каждой порождающей матрицы существует единственная проверочная матрица. Она повторяет правую часть порождающей матрицы и содержит в последних 3 строках единичную матрицу. Порождающая и проверочная матрицы являются взаимно перпендикулярными, то есть при их умножении получается нуль-матрица.

$$G \times H = 0 \quad (37)$$

Правая часть матрицы G может иметь разный порядок строк, главное, чтобы, во-первых, данный фрагмент был аналогичен части матрицы H , во-вторых, состоял только из строчек, в которых количество единиц не меньше 2, иначе в матрице H появятся линейно зависимые (одинаковые) строки. (**ПОЧЕМУ ЭТО ПЛОХО?**)

s – синдромный вектор (синдром) размера $(n - k)$.

$$s = Y \times H \quad (38)$$

Можем вычислить ошибку: *ошибочный разряд соответствует номеру строки (если считать с 1) порождающей матрицы с вычисленным синдромом*. Таким образом, код Хэмминга позволяет исправлять ошибки в полученных сообщениях. Если синдром является нулевым вектором, значит, с высокой вероятностью ошибки нет.

3.2 Кодирование

Зададим матрицу G , согласно требованиям к ней, описанным выше.

$$G^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (39)$$

Сразу запишем проверочную матрицу H

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (40)$$

Проведем кодирование слова **COBA** (*10001 01110 00010 00000*)

4 Задание 4. Код Хэмминг?