

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 Теоретическая справка

Шифр Хилла – полиграммный шифр подстановки, основанные на линейной алгебре и модульной арифметике.

1. Сначала составляется используемый алфавит, используемые символы нумеруются, размер алфавита n ;
2. Задается сообщение, которое нужно зашифровать;
3. Задается матрица ключа размера $m \times m$, удовлетворяющая требованиям:
 - а) определитель не может быть равным 0, то есть матрица ключа должна быть обратима;
 - б) определитель не может иметь общих делителей с n – размером алфавита;
4. Заданное ранее сообщение разбивается на блоки по m символов и рассматривается как m - мерный вектор;
5. Матрица ключа последовательно умножается по модулю n на каждый из полученных векторов.

Общая формула шифрования:

Пусть P и C – векторы столбцы высоты m , представляющие открытый и зашифрованный текст соответственно, K – матрица $m \times m$, представляющая ключ шифрования. Операции выполняются по модулю n .

$$KP(\text{mod } n) = C \quad (1)$$

Общая формула расшифрования:

$$K^{-1}C(\text{mod } n) = P \quad (2)$$

здесь обратная матрица ключа K^{-1} вычисляется по модулю n .

1.2 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
Е	3	П	7		

Сообщение для шифрования: **ЗВЕЗДНАЯПЫЛЬ**

Размер алфавита в нашем случае:

$$n = 11$$

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

1.3 Шифрование с помощью матрицы-ключа 2×2

Матрица-ключ размера 2×2 :

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \quad (3)$$

Проверка определителя:

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

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

Далее представлены фрагменты сообщения и соответствующие векторы кодов:

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

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

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 4 \\ 1 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 25 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 3 \end{pmatrix} \quad (5)$$

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 3 \\ 4 \end{pmatrix} \pmod{11} = \begin{pmatrix} 11 \\ 48 \end{pmatrix} \pmod{11} = \begin{pmatrix} 0 \\ 4 \end{pmatrix} \quad (6)$$

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

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 0 \\ 10 \end{pmatrix} \pmod{11} = \begin{pmatrix} 20 \\ 90 \end{pmatrix} \pmod{11} = \begin{pmatrix} 9 \\ 2 \end{pmatrix} \quad (8)$$

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

$$\begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \times \begin{pmatrix} 5 \\ 9 \end{pmatrix} \pmod{11} = \begin{pmatrix} 23 \\ 101 \end{pmatrix} \pmod{11} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad (10)$$

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: **HEAZEPBVDVVD**

1.4 Шифрование с помощью матрицы-ключа 3×3

Матрица-ключ размера 3×3 :

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad (11)$$

Проверка определителя:

$$\begin{vmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{vmatrix} = 1 \neq 0 \quad (12)$$

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

$$\mathbf{ZBE} \rightarrow \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} ;$$

$$\mathbf{ZDH} \rightarrow \begin{pmatrix} 4 \\ 2 \\ 6 \end{pmatrix} ; \mathbf{AEP} \rightarrow \begin{pmatrix} 0 \\ 10 \\ 7 \end{pmatrix} ;$$

$$\mathbf{BVL} \rightarrow \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix}$$

Повторяем действия, описанные в разделе 1.2:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} \quad (13)$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 4 \\ 2 \\ 6 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 6 \\ 10 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 6 \\ 10 \end{pmatrix} \quad (14)$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 10 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 10 \\ 7 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 10 \\ 7 \\ 7 \end{pmatrix} \quad (15)$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix} \pmod{11} = \begin{pmatrix} 13 \\ 9 \\ 17 \end{pmatrix} \pmod{11} = \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix} \quad (16)$$

Декодируем:

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

Полученное сообщение: **ЛЕПННЯЯППДЬН**

1.5 Шифрование с помощью матрицы-ключа 4×4

Матрица-ключ размера 4×4 :

$$C = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \quad (17)$$

Проверка определителя:

$$\begin{vmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{vmatrix} = -1 \neq 0 \quad (18)$$

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

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

Повторяем действия, описанные в разделе 1.2:

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

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 18 \\ 0 \\ 12 \\ 8 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 7 \\ 0 \\ 1 \\ 8 \end{pmatrix} \quad (20)$$

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

Декодируем:

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

Полученное сообщение: **БЕАЛПАВЫДЛЯЗ**

1.6 Имитация вредоносного вмешательства

а) Повредим фразу, полученную в пункте 1.2

Таблица 2 – Повреждение первого результата

Исходные символы	Н	Ё	А	З	Е	П	Ь	Д	В	В	В	Д
После атаки	Н	Л	А	З	Ь	П	Ь	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:

$$A^{-1} = \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix}^{-1} \pmod{11} = \begin{pmatrix} 9 & 9 \\ 7 & 1 \end{pmatrix} \quad (22)$$

Разобьем фразу **НЛАЗЬПДЫВВД** на фрагменты:

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

Расшифруем сообщение:

$$\begin{pmatrix} 9 & 9 \\ 7 & 1 \end{pmatrix} \times \begin{pmatrix} 6 \\ 5 \end{pmatrix} \pmod{11} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \quad (23)$$

$$\begin{pmatrix} 9 & 9 \\ 7 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 4 \end{pmatrix} \pmod{11} = \begin{pmatrix} 3 \\ 4 \end{pmatrix} \quad (24)$$

$$\begin{pmatrix} 9 & 9 \\ 7 & 1 \end{pmatrix} \times \begin{pmatrix} 9 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \quad (25)$$

$$\begin{pmatrix} 9 & 9 \\ 7 & 1 \end{pmatrix} \times \begin{pmatrix} 9 \\ 2 \end{pmatrix} \pmod{11} = \begin{pmatrix} 0 \\ 10 \end{pmatrix} \quad (26)$$

$$\begin{pmatrix} 9 & 9 \\ 7 & 1 \end{pmatrix} \times \begin{pmatrix} 8 \\ 1 \end{pmatrix} \pmod{11} = \begin{pmatrix} 4 \\ 2 \end{pmatrix} \quad (27)$$

$$\begin{pmatrix} 9 & 9 \\ 7 & 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ 2 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \quad (28)$$

Декодируем полученный результат:

$$\begin{aligned} \begin{pmatrix} 0 \\ 3 \end{pmatrix} &\rightarrow \mathbf{АЕ}; \begin{pmatrix} 3 \\ 4 \end{pmatrix} \rightarrow \mathbf{ЕЗ}; \begin{pmatrix} 1 \\ 4 \end{pmatrix} \rightarrow \mathbf{ВЗ}; \begin{pmatrix} 0 \\ 10 \end{pmatrix} \rightarrow \mathbf{АЯ}; \\ \begin{pmatrix} 4 \\ 2 \end{pmatrix} &\rightarrow \mathbf{ЗД}; \begin{pmatrix} 5 \\ 9 \end{pmatrix} \rightarrow \mathbf{ЛЬ} \end{aligned}$$

Полученное сообщение: **АЕ ЕЗ ВЗ АЯ ЗД ЛЬ**

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	Е	П	Н	Н	Я	Я	П	П	Д	Ь	Н
После атаки	Л	Е	П	Н	Ы	А	Я	В	П	Д	Ь	Н
Коды после атаки	5	3	7	6	8	0	10	1	7	2	9	6

Найдем обратную матрицу от второго ключа:

$$B^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}^{-1} \pmod{11} = \begin{pmatrix} 0 & 10 & 1 \\ 1 & 1 & 10 \\ 0 & 1 & 0 \end{pmatrix} \quad (29)$$

Разобьем фразу **ЛЕПНЫАЯВПДЬН** на фрагменты:

$$\begin{aligned} \mathbf{ЛЕП} &\rightarrow \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix}; \\ \mathbf{НЫА} &\rightarrow \begin{pmatrix} 6 \\ 8 \\ 0 \end{pmatrix}; \quad \mathbf{ЯВП} \rightarrow \begin{pmatrix} 10 \\ 1 \\ 7 \end{pmatrix}; \\ \mathbf{ДЬН} &\rightarrow \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix} \end{aligned}$$

Расшифруем сообщение:

$$\begin{pmatrix} 0 & 10 & 1 \\ 1 & 1 & 10 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \quad (30)$$

$$\begin{pmatrix} 0 & 10 & 1 \\ 1 & 1 & 10 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 6 \\ 8 \\ 0 \end{pmatrix} \pmod{11} = \begin{pmatrix} 3 \\ 3 \\ 8 \end{pmatrix} \quad (31)$$

$$\begin{pmatrix} 0 & 10 & 1 \\ 1 & 1 & 10 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 10 \\ 1 \\ 7 \end{pmatrix} \pmod{11} = \begin{pmatrix} 6 \\ 4 \\ 1 \end{pmatrix} \quad (32)$$

$$\begin{pmatrix} 0 & 10 & 1 \\ 1 & 1 & 10 \\ 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix} \pmod{11} = \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix} \quad (33)$$

Декодируем полученный результат:

$$\begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \rightarrow \mathbf{ЗВЕ} ; \begin{pmatrix} 3 \\ 3 \\ 8 \end{pmatrix} \rightarrow \mathbf{ЕЕЫ} ; \begin{pmatrix} 6 \\ 4 \\ 1 \end{pmatrix} \rightarrow \mathbf{НЗВ} ; \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix} \rightarrow \mathbf{ЫЛЬ}$$

Полученное сообщение: **ЗВЕ ЕЕЫ 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	Е	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:

$$C^{-1} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}^{-1} \pmod{11} = \begin{pmatrix} 10 & 10 & 1 & 1 \\ 1 & 1 & 10 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 10 \end{pmatrix} \quad (34)$$

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

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

Повторим привычные действия для расшифровки сообщения:

$$\begin{pmatrix} 10 & 10 & 1 & 1 \\ 1 & 1 & 10 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 10 \end{pmatrix} \times \begin{pmatrix} 1 \\ 7 \\ 0 \\ 2 \end{pmatrix} \pmod{11} = \begin{pmatrix} 5 \\ 8 \\ 7 \\ 10 \end{pmatrix} \quad (35)$$

$$\begin{pmatrix} 10 & 10 & 1 & 1 \\ 1 & 1 & 10 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 10 \end{pmatrix} \times \begin{pmatrix} 7 \\ 0 \\ 1 \\ 8 \end{pmatrix} \pmod{11} = \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix} \quad (36)$$

$$\begin{pmatrix} 10 & 10 & 1 & 1 \\ 1 & 1 & 10 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 10 \end{pmatrix} \times \begin{pmatrix} 2 \\ 5 \\ 10 \\ 4 \end{pmatrix} \pmod{11} = \begin{pmatrix} 7 \\ 8 \\ 6 \\ 9 \end{pmatrix} \quad (37)$$

Декодируем полученный результат:

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

Полученное сообщение: **ЛЫПЯ ДНАЯПЫЛЬ**

1.7 Программное решение

Также для решения задания 1 была написана программа на *Java*, которая предназначена для шифрования и расшифровки заданных сообщений и ключей размером 2×2 , 3×3 , 4×4 . В конце документа в приложении 1 приведены примеры работы программы с заданными "красивыми" ключами: **ЛАНЬ**, **ИВАНЯВАНЯ**, **ЛЕДЗАЛЕНВЫДАЛПАН**

1.8 Вывод

На практике убедилась в том, что алгоритм Хилла работает. На мой взгляд, эффективнее разбивать сообщение на блоки минимального размера, так как в случае "взлома" сообщения и изменения какого-то конкретного символа не удастся расшифровать целый блок символов, в котором была повреждена 1 буква.

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:

$$Y = X \times G(\text{mod}2) \quad (38)$$

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.

$$G \times H = 0 \quad (39)$$

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 $(n - k)$.

$$s = Y \times H \quad (40)$$

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.

$$G^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (41)$$

Сразу запишем проверочную матрицу H

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (42)$$

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

4 Задание 4. Код Хэмминг?

5 Приложение 1



```
Encryption x
C:\Users\user\.jdk\openjdk-20.0.1\bin\java.exe
Добро пожаловать ^.^
Введите фразу из 12 символов для шифрования:
ЗВЕЗДНАЯПЫЛЬ
Фраза для шифрования: ЗВЕЗДНАЯПЫЛЬ
В алфавите символов: 11
| Код | Символ |
-----
| 0 | А |
-----
| 1 | В |
-----
| 2 | Д |
-----
| 3 | Е |
-----
| 4 | З |
-----
| 5 | Л |
-----
| 6 | Н |
-----
| 7 | П |
-----
| 8 | Ы |
-----
| 9 | Ъ |
-----
| 10 | Я |
```

а)

```
-----  
| 10 | я |  
-----  
  
Выберите размерность ключа:  
2 -- для матрицы 2 x 2;  
3 -- для матрицы 3 x 3;  
4 -- для матрицы 4 x 4;  
3  
  
Введите фразу для ключа из 4 символов алфавита выше  
ПАНЬ  
  
Разобьем фразу ЗВЕЗДНАЯПЬЛЬ на фрагменты по 2 символа и запишем соответствующие коды:  
ЗВ -> 4 1  
ЕЗ -> 3 4  
ДН -> 2 6  
АЯ -> 0 10  
ПЫ -> 7 8  
ЛЬ -> 5 9  
  
Проведем матричное умножение ключа на каждый вектор-фрагмент фразы и возьмем результат по модулю 11:  
4 9 -> Ь  
1 -> 0 -> А  
  
-----  
3 4 -> З  
4 -> 10 -> Я  
  
-----  
2 10 -> Я  
6 -> 0 -> А  
  
-----  
0 0 -> А  
10 -> 2 -> Д  
  
-----  
7 2 -> П
```

б)

```
-----
7      2 -> Д
8 -> 4 -> З
-----
5      3 -> Е
9 -> 1 -> В
-----

В результате шифрования получим фразу: БАЗЯЯАДДЗЕВ
Выберите дальнейшие действия:
1 -- Расшифровать полученное сообщение;
2 -- Повредить полученное сообщение;
3 -- Зашифровать фразу другим ключом;
2
Начальная фраза: ЗВЕЗДНАЯПЫЛЬ
Зашифрованная фраза: БАЗЯЯАДДЗЕВ
Введите поврежденную фразу:
НЗАЯЯАДДЗЕВ
Расшифровать (1 / 0)? НЗАЯЯАДДЗЕВ
1
Разобьем фразу НЗАЯЯАДДЗЕВ на фрагменты по 2 символа и запишем соответствующие коды:
НЗ -> 6 4
АЯ -> 0 10
ЯА -> 10 0
АД -> 0 2
ДЗ -> 2 4
ЕВ -> 3 1
Найдем обратную по модулю 11 матрицу ключа.
Матрица ключа выглядела так:
5 0
6 9
Обратная по модулю 11 матрица ключа:
```

в)

```
системы
ЦЗ -> 2 4
ЕВ -> 3 1
Найдем обратную по модулю 11 матрицу ключа.
Матрица ключа выглядела так:
5 0
6 9
Обратная по модулю 11 матрица ключа:
9 0
5 5
Проведем матричное умножение обратной матрицы ключа на каждый вектор-фрагмент фразы и возьмем результат по модулю 11:
6 10 -> Я
4 -> 6 -> Н
-----
0 0 -> А
10 -> 6 -> Н
-----
10 2 -> Д
0 -> 6 -> Н
-----
0 0 -> А
2 -> 10 -> Я
-----
2 7 -> П
4 -> 8 -> Ы
-----
3 5 -> Л
1 -> 9 -> Ъ
-----
В результате дешифрования получим фразу: ЯНАНДНАЯПЫЛЬ
Начальная фраза: ЗВЕЗДНАЯПЫЛЬ
```

г)

Рис. 1. Результаты работы программы для ключа 2×2 .