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: ***ЗВЁЗДНАЯПЫЛЬ***
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 :

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \tag{1}$$

Проверка определителя:

$$\begin{vmatrix} 1 & 2 \\ 4 & 9 \end{vmatrix} = 1 \neq 0 \tag{2}$$

Запишем фразу, подлежащую шифрования с помощью кодов символов алфавита и разобьем наше сообщение на векторы.
Далее представлены фрагменты сообщения и соотвествующие векторы кодов:

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

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

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

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

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

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

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

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

Декодируем полученный результат:

$$\begin{pmatrix}6\\3\end{pmatrix} \to \textbf{\textit{НЁ}}\ ;\ \begin{pmatrix}0\\4\end{pmatrix} \to \textbf{\textit{АЗ}}\ ;\ \begin{pmatrix}3\\7\end{pmatrix} \to \textbf{\textit{ЁП}}\ ;\ \begin{pmatrix}9\\2\end{pmatrix} \to \textbf{\textit{ЬД}}\ ;$$
$$\begin{pmatrix}1\\1\end{pmatrix} \to \textbf{\textit{ВВ}}\ ;\ \begin{pmatrix}1\\2\end{pmatrix} \to \textbf{\textit{ВД}}$$

Полученное сообщение: ***НЁАЗЁПЬДВВВД***

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 соотвествующие им векторы кодов:

$$\textbf{\textit{ЗВЁ}} \to \begin{pmatrix}4\\1\\3\end{pmatrix};$$

$$\textbf{\textit{ЗДН}} \to \begin{pmatrix}4\\2\\6\end{pmatrix}; \textbf{\textit{АЯП}} \to \begin{pmatrix}0\\10\\7\end{pmatrix};$$

$$\textbf{\textit{ЫЛЬ}} \to \begin{pmatrix}8\\5\\9\end{pmatrix}$$

Повторяем действия, описанные в разделе 1.2:

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

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

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

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

Декодируем:

$$\begin{pmatrix}5\\7\\3\end{pmatrix} \to \textbf{\textit{ЛПЁ}}; \begin{pmatrix}6\\6\\10\end{pmatrix} \to \textbf{\textit{ННЯ}}; \begin{pmatrix}10\\7\\7\end{pmatrix} \to \textbf{\textit{ЯПП}}; \begin{pmatrix}2\\9\\6\end{pmatrix} \to \textbf{\textit{ДЬН}}$$

Полученное сообщение: ***ЛПЁННЯЯППДЬН***

1.4 Шифрование с помощью матрицы-ключа 4×4

Матрица-ключ размера 4×4 :

$$C = \begin{pmatrix}1&1&0&1\\0&0&1&0\\1&0&1&1\\1&1&0&0\end{pmatrix} \tag{15}$$

Проверка определителя:

$$\begin{vmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{vmatrix} = -1 \neq 0 \tag{16}$$

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

$$\textbf{\textit{ЗВЁЗ}} \rightarrow \begin{pmatrix} 4 \\ 1 \\ 3 \\ 4 \end{pmatrix};$$

$$\textbf{\textit{ДНАЯ}} \rightarrow \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix};$$

$$\textbf{\textit{ПЫЛЬ}} \rightarrow \begin{pmatrix} 7 \\ 8 \\ 5 \\ 9 \end{pmatrix}$$

Повторяем действия, описанные в разделе 1.2:

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

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

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

Декодируем:

$$\begin{pmatrix}9\\3\\0\\5\end{pmatrix} \to \textbf{\textit{ЬЁАЛ}} \; ; \; \begin{pmatrix}7\\0\\1\\8\end{pmatrix} \to \textbf{\textit{ПАВЫ}} \; ; \; \begin{pmatrix}2\\5\\10\\4\end{pmatrix} \to \textbf{\textit{ДЛЯЗ}}$$

Полученное сообщение: ***ЬЁАЛПАВЫДЛЯЗ***

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	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:

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

Разобьем фразу ***НЛАЗЬПЬДЫВВД*** на фрагменты:

$$\textbf{\textit{НЛ}} \to \begin{pmatrix}6\\5\end{pmatrix} \; ; \; \textbf{\textit{АЗ}} \to \begin{pmatrix}0\\4\end{pmatrix} \; ; \; \textbf{\textit{ЬП}} \to \begin{pmatrix}9\\7\end{pmatrix} \; ; \; \textbf{\textit{ЬД}} \to \begin{pmatrix}9\\2\end{pmatrix};$$
$$\textbf{\textit{ЫВ}} \to \begin{pmatrix}8\\1\end{pmatrix} \; ; \; \textbf{\textit{ВД}} \to \begin{pmatrix}1\\2\end{pmatrix}$$

Расшифруем сообщение:

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

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

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

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

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

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

Декодируем полученный результат:

$$\begin{pmatrix} 0 \\ 3 \end{pmatrix} \to \textbf{\textit{АЁ}}\ ;\ \begin{pmatrix} 3 \\ 4 \end{pmatrix} \to \textbf{\textit{ЁЗ}}\ ;\ \begin{pmatrix} 1 \\ 4 \end{pmatrix} \to \textbf{\textit{ВЗ}}\ ;\ \begin{pmatrix} 0 \\ 10 \end{pmatrix} \to \textbf{\textit{АЯ}}\ ;$$
$$\begin{pmatrix} 4 \\ 2 \end{pmatrix} \to \textbf{\textit{ЗД}}\ ;\ \begin{pmatrix} 5 \\ 9 \end{pmatrix} \to \textbf{\textit{ЛЬ}}$$

Полученное сообщение: **АЁ ЁЗ 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	Ь	З	Я	Ё	А	Ь	Н	Ь	Д	А	З	В
После атаки	П	З	Я	Ё	Л	Ь	Н	Ь	Д	А	Ы	В
Коды после атаки	7	4	10	3	5	9	6	9	2	0	8	1

Найдем обратную матрицу от второго ключа:

$$\begin{pmatrix} 1 & 5 & 0 \\ 2 & 0 & 6 \\ 0 & 2 & 10 \end{pmatrix}^{-1} = \frac{1}{56} \begin{pmatrix} 6 & 25 & -15 \\ 10 & -5 & 3 \\ -28 & 1 & 5 \end{pmatrix} \tag{27}$$

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 третьеого ключа:

$$\begin{pmatrix} 5 & 3 & 2 & 4 \\ 0 & 5 & 3 & 6 \\ 1 & 8 & 2 & 0 \\ 5 & 7 & 0 & 6 \end{pmatrix}^{-1} = \frac{1}{433} \begin{pmatrix} 84 & -58 & 3 & 2 \\ -39 & -4 & 45 & 30 \\ 114 & 45 & 35 & -121 \\ -\frac{49}{2} & 53 & -55 & \frac{71}{2} \end{pmatrix} \tag{28}$$

2 Задание 2. Взлом шифра Хилла

3 Задание 3. Код Хэмминга

4 Задание 4. Код Хэмминг?