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 А 2×2 соотвествует ключевому слову: ***ЛАНЬ***

$$\begin{vmatrix} 5 & 0 \\ 6 & 9 \end{vmatrix} = 5 * 9 - 0 * 6 = 45 \tag{1}$$

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:

$$\begin{pmatrix} 5 & 0 \\ 6 & 9 \end{pmatrix} \times \begin{pmatrix} 4 \\ 1 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 20 \\ 33 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 9 \\ 0 \end{pmatrix} \tag{2}$$

$$\begin{pmatrix} 5 & 0 \\ 6 & 9 \end{pmatrix} \times \begin{pmatrix} 3 \\ 4 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 15 \\ 54 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 4 \\ 10 \end{pmatrix} \tag{3}$$

$$\begin{pmatrix}5 & 0\\6 & 9\end{pmatrix} \times \begin{pmatrix}2\\6\end{pmatrix} (mod\ 11) = \begin{pmatrix}10\\66\end{pmatrix} (mod\ 11) = \begin{pmatrix}10\\0\end{pmatrix} \quad (4)$$

$$\begin{pmatrix}5 & 0\\6 & 9\end{pmatrix} \times \begin{pmatrix}0\\10\end{pmatrix} (mod\ 11) = \begin{pmatrix}0\\90\end{pmatrix} (mod\ 11) = \begin{pmatrix}0\\2\end{pmatrix} \quad (5)$$

$$\begin{pmatrix}5 & 0\\6 & 9\end{pmatrix} \times \begin{pmatrix}7\\8\end{pmatrix} (mod\ 11) = \begin{pmatrix}35\\114\end{pmatrix} (mod\ 11) = \begin{pmatrix}2\\4\end{pmatrix} \quad (6)$$

$$\begin{pmatrix}5 & 0\\6 & 9\end{pmatrix} \times \begin{pmatrix}5\\9\end{pmatrix} (mod\ 11) = \begin{pmatrix}25\\111\end{pmatrix} (mod\ 11) = \begin{pmatrix}3\\1\end{pmatrix} \quad (7)$$

Декодируем полученный результат:

$$\begin{pmatrix}9\\0\end{pmatrix} \to \textbf{\textit{ЬА}}\ ;\ \begin{pmatrix}4\\10\end{pmatrix} \to \textbf{\textit{ЗЯ}}\ ;\ \begin{pmatrix}10\\0\end{pmatrix} \to \textbf{\textit{ЯА}}\ ;\ \begin{pmatrix}0\\2\end{pmatrix} \to \textbf{\textit{АД}}\ ;$$
$$\begin{pmatrix}2\\4\end{pmatrix} \to \textbf{\textit{ДЗ}}\ ;\ \begin{pmatrix}3\\1\end{pmatrix} \to \textbf{\textit{ЁВ}}$$

Полученное сообщение: ***ЬАЗЯЯААДДЗЁВ***

1.3 Шифрование с помощью матрицы-ключа 3×3

Матрица B 3×3 соотвествует ключевому слову: ***ВЛАДАНАДЯ***

$$\begin{vmatrix}1 & 5 & 0\\2 & 0 & 6\\0 & 2 & 10\end{vmatrix} = -112 \quad (8)$$

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:

$$\begin{pmatrix}1&5&0\\2&0&6\\0&2&10\end{pmatrix}\times\begin{pmatrix}4\\1\\3\end{pmatrix}(mod\ 11)=\begin{pmatrix}9\\26\\32\end{pmatrix}(mod\ 11)=\begin{pmatrix}9\\4\\10\end{pmatrix} \tag{9}$$

$$\begin{pmatrix}1&5&0\\2&0&6\\0&2&10\end{pmatrix}\times\begin{pmatrix}4\\2\\6\end{pmatrix}(mod\ 11)=\begin{pmatrix}14\\44\\64\end{pmatrix}(mod\ 11)=\begin{pmatrix}3\\0\\9\end{pmatrix} \tag{10}$$

$$\begin{pmatrix}1&5&0\\2&0&6\\0&2&10\end{pmatrix}\times\begin{pmatrix}0\\10\\7\end{pmatrix}(mod\ 11)=\begin{pmatrix}50\\42\\90\end{pmatrix}(mod\ 11)=\begin{pmatrix}6\\9\\2\end{pmatrix} \tag{11}$$

$$\begin{pmatrix}1&5&0\\2&0&6\\0&2&10\end{pmatrix}\times\begin{pmatrix}8\\5\\9\end{pmatrix}(mod\ 11)=\begin{pmatrix}33\\70\\100\end{pmatrix}(mod\ 11)=\begin{pmatrix}0\\4\\1\end{pmatrix} \tag{12}$$

Декодируем:

$$\begin{pmatrix}9\\4\\10\end{pmatrix}\rightarrow \textbf{\textit{ЬЗЯ}}\ ;\ \begin{pmatrix}3\\0\\9\end{pmatrix}\rightarrow \textbf{\textit{ЁАЬ}}\ ;\ \begin{pmatrix}6\\9\\2\end{pmatrix}\rightarrow \textbf{\textit{НЬД}}\ ;\ \begin{pmatrix}0\\4\\1\end{pmatrix}\rightarrow \textbf{\textit{АЗВ}}$$

Полученное сообщение: ***ЬЗЯЁАЬНЬДАЗВ***

1.4 Шифрование с помощью матрицы-ключа 4×4

Матрица С 4×4
соотвествует ключевому слову: ***ЛЁДЗАЛЁНВЫДАЛПАН***

$$\begin{vmatrix}5&3&2&4\\0&5&3&6\\1&8&2&0\\5&7&0&6\end{vmatrix}=-866 \tag{13}$$

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:

$$\begin{pmatrix} 5 & 3 & 2 & 4 \\ 0 & 5 & 3 & 6 \\ 1 & 8 & 2 & 0 \\ 5 & 7 & 0 & 6 \end{pmatrix} \times \begin{pmatrix} 4 \\ 1 \\ 3 \\ 4 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 45 \\ 38 \\ 18 \\ 51 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 1 \\ 5 \\ 7 \\ 7 \end{pmatrix} \quad (14)$$

$$\begin{pmatrix} 5 & 3 & 2 & 4 \\ 0 & 5 & 3 & 6 \\ 1 & 8 & 2 & 0 \\ 5 & 7 & 0 & 6 \end{pmatrix} \times \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 68 \\ 90 \\ 50 \\ 112 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 2 \\ 2 \\ 6 \\ 2 \end{pmatrix} \quad (15)$$

$$\begin{pmatrix} 5 & 3 & 2 & 4 \\ 0 & 5 & 3 & 6 \\ 1 & 8 & 2 & 0 \\ 5 & 7 & 0 & 6 \end{pmatrix} \times \begin{pmatrix} 7 \\ 8 \\ 5 \\ 9 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 105 \\ 109 \\ 81 \\ 145 \end{pmatrix} (mod\ 11) = \begin{pmatrix} 6 \\ 10 \\ 4 \\ 2 \end{pmatrix} \quad (16)$$

Декодируем:

$$\begin{pmatrix} 1 \\ 5 \\ 7 \\ 7 \end{pmatrix} \rightarrow \textbf{\textit{ВЛПП}};\ \begin{pmatrix} 2 \\ 2 \\ 6 \\ 2 \end{pmatrix} \rightarrow \textbf{\textit{ДДНД}};\ \begin{pmatrix} 6 \\ 10 \\ 4 \\ 2 \end{pmatrix} \rightarrow \textbf{\textit{НЯЗД}}$$

Полученное сообщение: ***ВЛППДДНДНЯЗД***

1.5 Имитация вредоносного вмешательства

а) Повредим фразу, полученную в пункте 1.2

Таблица 2 – Повреждение первого результата

Исходные символы	Ь	А	З	Я	Я	А	А	Д	Д	З	Ё	В
После атаки	Ь	А	З	Я	Н	А	П	Д	Ы	З	Ё	В
Коды после атаки	9	0	4	10	6	0	7	2	8	4	3	1

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

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

2 Задание 2. Взлом шифра Хилла

3 Задание 3. Код Хэмминга

4 Задание 4. Код Хэмминг?