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 соотвественно, K – матрица $m \times m$, представляющая ключ шифрования. Операции выполняются по модулю n.

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

Общая формула расшифрования:

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

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 :

$$A = \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix} \tag{3}$$

Проверка определителя:

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

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

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

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

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

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

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

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

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

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

Декодируем полученный результат:

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

Полученное сообщение: ***НЕАЗЕПЬДВВВД***

1.4 Шифрование с помощью матрицы-ключа 3×3

Матрица-ключ размера 3×3 :

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \tag{11}$$

Проверка определителя:

$$\begin{vmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{vmatrix} = 1 \neq 0 \tag{12}$$

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

$$\textbf{\textit{ЗВЕ}} \to \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \ ;$$
$$\textbf{\textit{ЗДН}} \to \begin{pmatrix} 4 \\ 2 \\ 6 \end{pmatrix} \ ; \textbf{\textit{АЯП}} \to \begin{pmatrix} 0 \\ 10 \\ 7 \end{pmatrix} \ ;$$
$$\textbf{\textit{ЫЛЬ}} \to \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix}$$

Повторяем действия, описанные в разделе 1.2:

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

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

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

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

Декодируем:

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

Полученное сообщение: ***ЛЕПННЯЯППДЬН***

1.5 Шифрование с помощью матрицы-ключа 4×4

Матрица-ключ размера 4×4 :

$$C=\begin{pmatrix}1&1&0&1\\0&0&1&0\\1&0&1&1\\1&1&0&0\end{pmatrix}\tag{17}$$

Проверка определителя:

$$\begin{vmatrix}1&1&0&1\\0&0&1&0\\1&0&1&1\\1&1&0&0\end{vmatrix}=-1\neq 0\tag{18}$$

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

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

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

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

Повторяем действия, описанные в разделе 1.2:

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

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

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

Декодируем:

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

Полученное сообщение: ***ЬЕАЛПАВЫДЛЯЗ***

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:

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

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

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

Расшифруем сообщение:

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

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

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

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

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

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

Декодируем полученный результат:

$$\begin{pmatrix} 0 \\ 3 \end{pmatrix} \to \boldsymbol{АЕ};\ \begin{pmatrix} 3 \\ 4 \end{pmatrix} \to \boldsymbol{ЕЗ};\ \begin{pmatrix} 1 \\ 4 \end{pmatrix} \to \boldsymbol{ВЗ};\ \begin{pmatrix} 0 \\ 10 \end{pmatrix} \to \boldsymbol{АЯ};$$
$$\begin{pmatrix} 4 \\ 2 \end{pmatrix} \to \boldsymbol{ЗД};\ \begin{pmatrix} 5 \\ 9 \end{pmatrix} \to \boldsymbol{ЛЬ}$$

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:

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

Разобьем фразу ***ЛЕПНЫАЯВПДЬН*** на фрагменты:

$$\textbf{\textit{ЛЕП}} \to \begin{pmatrix} 5 \\ 3 \\ 7 \end{pmatrix};$$

$$\textbf{\textit{НЫА}} \to \begin{pmatrix} 6 \\ 8 \\ 0 \end{pmatrix}; \ \textbf{\textit{ЯВП}} \to \begin{pmatrix} 10 \\ 1 \\ 7 \end{pmatrix};$$

$$\textbf{\textit{ДЬН}} \to \begin{pmatrix} 2 \\ 9 \\ 6 \end{pmatrix}$$

Расшифруем сообщение:

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

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

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

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

Декодируем полученный результат:

$$\begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix} \to \textbf{\textit{ЗВЕ}}\ ;\ \begin{pmatrix} 3 \\ 3 \\ 8 \end{pmatrix} \to \textbf{\textit{ЕЕЫ}}\ ;\ \begin{pmatrix} 6 \\ 4 \\ 1 \end{pmatrix} \to \textbf{\textit{НЗВ}}\ ;\ \begin{pmatrix} 8 \\ 5 \\ 9 \end{pmatrix} \to \textbf{\textit{ЫЛЬ}}$$

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	Ь	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 третьеого ключа:

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

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

$$\textbf{\textit{ВПАД}} \to \begin{pmatrix} 1 \\ 7 \\ 0 \\ 2 \end{pmatrix}\ ;$$

$$\textbf{\textit{ПАВЫ}} \to \begin{pmatrix} 7 \\ 0 \\ 1 \\ 8 \end{pmatrix}\ ;$$

$$\textbf{\textit{ДЛЯЗ}} \to \begin{pmatrix} 2 \\ 5 \\ 10 \\ 4 \end{pmatrix}$$

Повторим привычные действия для расшифровки сообщения:

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

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

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

Декодируем полученный результат:

$$\begin{pmatrix} 5 \\ 8 \\ 7 \\ 10 \end{pmatrix} \to \textbf{\textit{ЛЫПЯ}}\ ; \begin{pmatrix} 2 \\ 6 \\ 0 \\ 10 \end{pmatrix} \to \textbf{\textit{ДНАЯ}}\ ; \begin{pmatrix} 7 \\ 8 \\ 6 \\ 9 \end{pmatrix} \to \textbf{\textit{ПЫЛЬ}}\ ;$$

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 удается 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***. Соотвествующий 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:

$$Y = X \times G(mod2) \tag{38}$$

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.

$$G \times H = 0 \tag{39}$$

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).

$$s = Y \times H \tag{40}$$

Можем вычислить ошибку: ***ошибочный разряд соотвествует 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.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{41}$$

Сразу запишем проверочную матрицу H

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{42}$$

Проведем кодирование слова ***СОВА*** (***10001 01110 00010 00000***).
Перепишем код в блоки по 4 символа, чтобы мы смогли воспользоваться алгоритмом, получим ***1000 1011 1000 0100 0000***

Заметим, что для облегчения умножения "на листочке"можно пользоваться следующим правилом, вытекающим из самого определения матричного умножения:
ответом является вектор, состоящий из суммы строк матрицы G, номера которых (сверху 1 строка, ниже 2 и т.д.) соответсвуют номерам столбцов, в которых стоят 1, вектора кодируемой порции данных.

Вычисленная ниже матрица это наглядно иллюстрирует: 1 стоит в 1 столбце кодируемого вектора, результатом умножения является 1 строка матрицы G.

$$\begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix} \times \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\\ 0 & 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\end{pmatrix} \tag{43}$$

$$\begin{pmatrix}1 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\\ 0 & 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 0 & 1 & 1 & 0 & 1 & 0\end{pmatrix} \tag{44}$$

$$\begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix} \times \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\\ 0 & 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\end{pmatrix} \tag{45}$$

$$\begin{pmatrix}0 & 1 & 0 & 0\end{pmatrix} \times \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\\ 0 & 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 1 & 0 & 0 & 1 & 0 & 1\end{pmatrix} \tag{46}$$

$$\begin{pmatrix}0 & 0 & 0 & 0\end{pmatrix} \times \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\\ 0 & 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix} \tag{47}$$

В результате кодирования получаем:
10000 11101 10101 00001 10100 10100 00000 или соотвественно в виде текста: ***РЭХБФФА***

3.3 Имитация вредоносного вмешательства и декодирование для 1 бита

Вернемся к нашему закодированному сообщению: ***10 0 0011 1011010 1000011 0100101 0000000*** и заменим в нем третий бит на противоположный ***10 1 0011 1011010 1000011 0100101 0000000***.
С помощью проверочной матрицы H найдем ошибочный бит в сообщении, умножив каждый вектор закодированного сообщения длины 7 на H по модулю 2:

$$\begin{pmatrix}1 & 0 & 1 & 0 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 1 & 0\end{pmatrix} \tag{48}$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему в 3 строке матрицы H. Значит, ошибочным битом является 3 бит в данном фрагменте сообщения.
Далее убедимся, что в остальных фрагментах сообщения, не допущена ошибка.

$$\begin{pmatrix}1 & 0 & 1 & 1 & 0 & 1 & 0\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \tag{49}$$

$$\begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \tag{50}$$

$$\begin{pmatrix}0 & 1 & 0 & 0 & 1 & 0 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \tag{51}$$

$$\begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \tag{52}$$

Для всех фрагментов, кроме первого, синдромные векторы получились нулевыми, значит, в них нет ошибки.
Исправим ошибку и получим: ***10000 11101 10101 00001 10100 10100 00000***

3.4 Имитация вредоносного вмешательства и декодирование для 2 бит

Заметим, что вектор-синдром способен помочь в исправлении только 1 ошибки в отдельном фрагменте сообщения, если ошибок будет больше синдром с большой долей вероятности не будет нулевым, однако его указание на конкретный бит в данном случае может быть ошибочно.
Итак, заменим на противоположные по 1 биту в 2 фрагментах сообщения: ***10 0 0011 101101 0 1000011 0100101 0000000*** и заменим в нем третий и четырнадцатый биты на противоположные ***10 1 0011 101101 1 1000011 0100101 0000000***.

$$\begin{pmatrix}1 & 0 & 1 & 0 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 1 & 0\end{pmatrix} \tag{53}$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему в 3 строке матрицы H. Значит, ошибочным битом является 3 бит в данном фрагменте сообщения.

$$\begin{pmatrix}1 & 0 & 1 & 1 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 1\end{pmatrix} \tag{54}$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему в 7 строке матрицы H. Значит, ошибочным битом является 7 бит в данном фрагменте сообщения (14 для всего сообщения).

$$\begin{pmatrix}1 & 0 & 0 & 0 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \tag{55}$$

$$\begin{pmatrix}0 & 1 & 0 & 0 & 1 & 0 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \tag{56}$$

$$\begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \tag{57}$$

Исправим ошибки и получим: ***10000 11101 10101 00001 10100 10100 00000***

3.5 Имитация вредоносного вмешательства и декодирование для 3 бит

Заменим на противоположные по 1 биту в 3 фрагментах сообщения: ***1000011 1011010 1000011 0100101 0000000*** и заменим в нем третий, четырнадцатый и шестнадцатый биты на противоположные ***1010011 1011011 1100011 0100101 0000000***.
Поиск ошибочных битов:

$$\begin{pmatrix}1 & 0 & 1 & 0 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\1 & 0 & 1\\1 & 1 & 0\\1 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 1 & 0\end{pmatrix} \tag{58}$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему в 3 строке матрицы H. Значит, ошибочным битом является 3 бит в данном фрагменте сообщения.

$$\begin{pmatrix}1 & 0 & 1 & 1 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\1 & 0 & 1\\1 & 1 & 0\\1 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 1\end{pmatrix} \tag{59}$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему в 7 строке матрицы H. Значит, ошибочным битом является 7 бит в данном фрагменте сообщения (14 для всего сообщения).

$$\begin{pmatrix}1 & 1 & 0 & 0 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\1 & 0 & 1\\1 & 1 & 0\\1 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 0 & 1\end{pmatrix} \tag{60}$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему во 2 строке матрицы H. Значит, ошибочным битом является 2 бит в данном фрагменте сообщения (16 для всего сообщения).

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (mod\ 2) = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \tag{61}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (mod\ 2) = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \tag{62}$$

Исправим ошибки и получим: ***10000 11101 10101 00001 10100 10100 00000***

3.6 Имитация вредоносного вмешательства и декодирование для 4 бит

Заменим на противоположные по 1 биту в 4 фрагментах сообщения: ***10 0 0011 101101 0 1 0 00011 0100101 000000 0*** и заменим в нем 3, 14, 16 и 35 биты на противоположные ***10 1 0011 101101 1 1 1 00011 0100101 000000 1***.

Поиск ошибочных битов:

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} (mod\ 2) = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \tag{63}$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему в 3 строке матрицы H. Значит, ошибочным битом является 3 бит в данном фрагменте сообщения.

$$\begin{pmatrix}1 & 0 & 1 & 1 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\1 & 0 & 1\\1 & 1 & 0\\1 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 1\end{pmatrix} \quad (64)$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему в 7 строке матрицы H. Значит, ошибочным битом является 7 бит в данном фрагменте сообщения (14 для всего сообщения).

$$\begin{pmatrix}1 & 1 & 0 & 0 & 0 & 1 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\1 & 0 & 1\\1 & 1 & 0\\1 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}1 & 0 & 1\end{pmatrix} \quad (65)$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему во 2 строке матрицы H. Значит, ошибочным битом является 2 бит в данном фрагменте сообщения (16 для всего сообщения).

$$\begin{pmatrix}0 & 1 & 0 & 0 & 1 & 0 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\1 & 0 & 1\\1 & 1 & 0\\1 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 0\end{pmatrix} \quad (66)$$

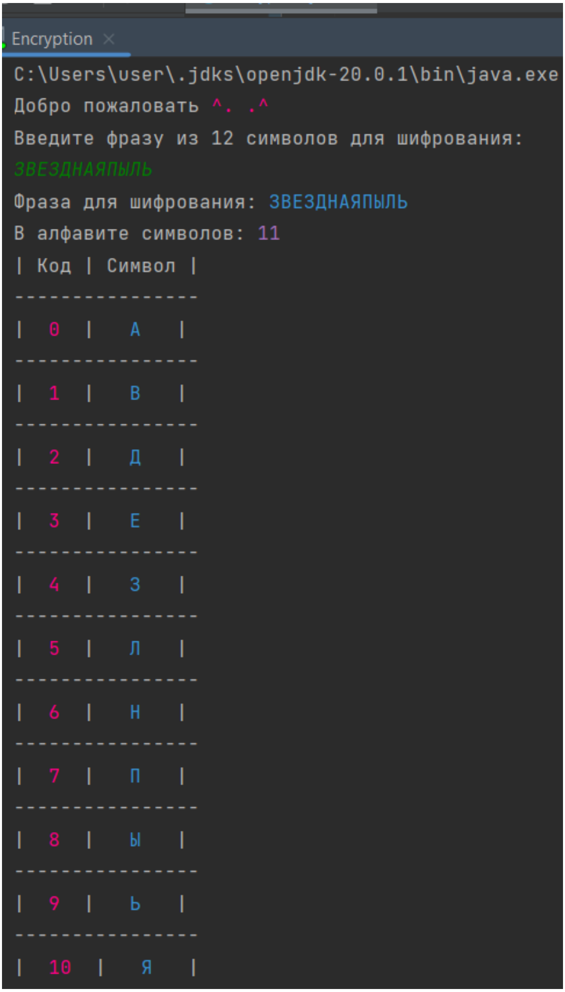
$$\begin{pmatrix}0 & 0 & 0 & 0 & 0 & 0 & 1\end{pmatrix} \times \begin{pmatrix}0 & 1 & 1\\1 & 0 & 1\\1 & 1 & 0\\1 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{pmatrix} (mod\ 2) = \begin{pmatrix}0 & 0 & 1\end{pmatrix} \quad (67)$$

В результате мы получили вектор (синдромный), соотвествующий набору, стоящему во 7 строке матрицы H. Значит, ошибочным битом является 7 бит в данном фрагменте сообщения (35 для всего сообщения).

Исправим ошибки и получим: ***10000 11101 10101 00001 10100 10100 00000***

4 Задание 4. Код Хэмминг?

5 Приложение 1



```
Encryption
C:\Users\user\.jdks\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  |   Ь   |
----------------
|  10  |   Я   |
```

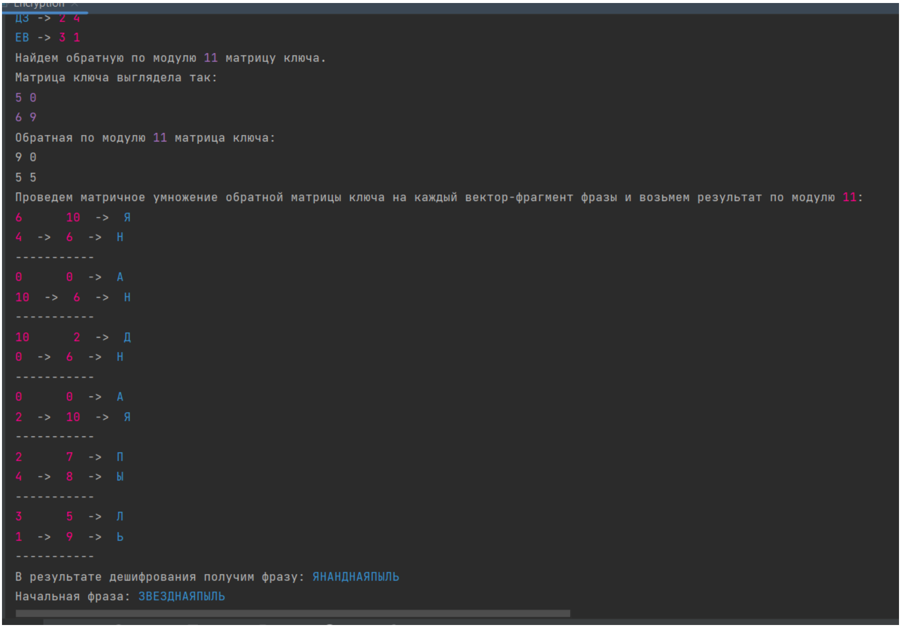
a)

```
----------------
|  10  |   Я   |
----------------
Выберите размерность ключа:
 2 -- для матрицы 2 x 2;
 3 -- для матрицы 3 x 3;
 4 -- для матрицы 4 x 4;
2
Введите фразу для ключа из 4 символов алфавита выше
ЛАНЬ
Разобьем фразу ЗВЕЗДНАЯПЫЛЬ на фрагменты по 2 символа и запишем соотвествующие 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: ЬАЗЯЯААДДЗЕВ
Выберите дальнейшие действия:
1 -- Расшифровать полученное сообщение;
2 -- Повредить полученное сообщение;
3 -- Зашифровать фразу другим ключем;
2
Начальная фраза: ЗВЕЗДНАЯПЫЛЬ
Зашифрованная фраза: ЬАЗЯЯААДДЗЕВ
Введите поврежденную фразу:
НЗАЯЯААДДЗЕВ
Расшифровать (1 / 0)? НЗАЯЯААДДЗЕВ
1
Разобьем фразу НЗАЯЯААДДЗЕВ на фрагменты по 2 символа и запишем соотвествующие 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)



```
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  ->  Ь
-----------
В результате дешифрования получим фразу: ЯНАНДНАЯПЫЛЬ
Начальная фраза: ЗВЕЗДНАЯПЫЛЬ
```

г)

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