Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»
(УНИВЕРСИТЕТ ИТМО)

Факультет «Систем управления и робототехники»

ОТЧЕТ
О ЛАБОРАТОРНОЙ РАБОТЕ № 1

По дисциплине «Практическая линейная алгебра»
на тему: «Кодирование и шифрование»

Студенты:
Гизбрехт В.Д. группа 1
Ли Х.С. группа 1
Лаврик В.В. группа 4

Проверил:
Догадин Е.В.

г. Санкт-Петербург
2024

Задание 1. Полиграммный шифр Хилла

1. Сопоставим Алфавиту численные значения

А	Б	В	Г	Д	Е	Ё	Ж	З	И
0	1	2	3	4	5	6	7	8	9
Й	К	Л	М	Н	О	П	Р	С	Т
10	11	12	13	14	15	16	17	18	19
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
20	21	22	23	24	25	26	27	28	29
Э	Ю	Я	space	.	!	?			
30	31	32	33	34	35	36			

Длина алфавита – 37 символов. 37 – простое число.
Простое число выбрано для того, чтобы детерминант матрицы ключа не имел общие делители с основанием модуля.

2. Выбираем сообщение для шифра

саламалейкум

3. Сопоставляем коды букв нашего сообщения

с	а	л	а	м	а	л	е	й	к	у	м
18	0	12	0	13	0	12	5	10	11	20	13

4. Условия выбора матрицы ключа

А. Детерминант не равен 0
Б. Детерминант не равен 37

5. Матрица-ключ 2x2

1) Выбор матрицы ключа:

$$K = \begin{matrix} 2 & 3 \\ 1 & 2 \end{matrix}$$

$$Det(K) = 2 * 2 - 1 * 3 = 1$$

$$K^{-1} = \begin{matrix} 2 & -3 \\ -1 & 2 \end{matrix} (mod\ 37)$$

Детерминант не равен 0 и 37, матрица обратима в целых числах, следовательно она нам подходит

2) **Кодирование матрицей 2x2**

Для кодирования мы берем вектор размерности 2 и умножаем матрицу-ключ на заданный вектор и получаем вектор размерности 2

Далее мы находим буквенный эквивалент и получаем зашифрованное сообщение

$$\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix} * \begin{bmatrix}18\\0\end{bmatrix} = \begin{bmatrix}36\\18\end{bmatrix} => \begin{bmatrix}36\\18\end{bmatrix}(mod\ 37) = \begin{bmatrix}36\\18\end{bmatrix} = \begin{bmatrix}?\\С\end{bmatrix}$$

$$\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix} * \begin{bmatrix}12\\0\end{bmatrix} = \begin{bmatrix}24\\12\end{bmatrix} => \begin{bmatrix}24\\12\end{bmatrix}(mod\ 37) = \begin{bmatrix}24\\12\end{bmatrix} = \begin{bmatrix}Ч\\Л\end{bmatrix}$$

$$\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix} * \begin{bmatrix}13\\0\end{bmatrix} = \begin{bmatrix}26\\13\end{bmatrix} => \begin{bmatrix}26\\13\end{bmatrix}(mod\ 37) = \begin{bmatrix}26\\13\end{bmatrix} = \begin{bmatrix}Щ\\М\end{bmatrix}$$

$$\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix} * \begin{bmatrix}12\\5\end{bmatrix} = \begin{bmatrix}39\\22\end{bmatrix} => \begin{bmatrix}39\\22\end{bmatrix}(mod\ 37) = \begin{bmatrix}2\\22\end{bmatrix} = \begin{bmatrix}В\\Х\end{bmatrix}$$

$$\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix} * \begin{bmatrix}10\\11\end{bmatrix} = \begin{bmatrix}53\\32\end{bmatrix} => \begin{bmatrix}53\\32\end{bmatrix}(mod\ 37) = \begin{bmatrix}16\\32\end{bmatrix} = \begin{bmatrix}П\\Я\end{bmatrix}$$

$$\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix} * \begin{bmatrix}20\\13\end{bmatrix} = \begin{bmatrix}79\\46\end{bmatrix} => \begin{bmatrix}79\\46\end{bmatrix}(mod\ 37) = \begin{bmatrix}5\\9\end{bmatrix} = \begin{bmatrix}Е\\И\end{bmatrix}$$

На выходе мы получаем закодированное сообщение:

?счлщмвхпяеи

3) **«Вредоносное вмешательство» и расшифровка**

Заменяем 3 символа в получившемся шифре:

бсчлщмвапяри = 1, 18, 24, 12, 26, 13, 2, 0, 16, 32, 17, 9

Умножаем обратную матрицу на вектор размерности 2 для получения ответа:

$$\begin{bmatrix}2 & -3\\-1 & 2\end{bmatrix}(mod\ 37) = \begin{bmatrix}2 & 34\\36 & 2\end{bmatrix}$$

$$\begin{bmatrix}2 & 34\\36 & 2\end{bmatrix} * \begin{bmatrix}1\\18\end{bmatrix} = \begin{bmatrix}578\\70\end{bmatrix} => \begin{bmatrix}578\\70\end{bmatrix}(mod\ 37) = \begin{bmatrix}22\\33\end{bmatrix} = \begin{bmatrix}Х\end{bmatrix}$$

$$\begin{bmatrix}2 & 34\\36 & 2\end{bmatrix} * \begin{bmatrix}24\\12\end{bmatrix} = \begin{bmatrix}456\\888\end{bmatrix} => \begin{bmatrix}456\\888\end{bmatrix}(mod\ 37) = \begin{bmatrix}12\\0\end{bmatrix} = \begin{bmatrix}Л\\М\end{bmatrix}$$

$$\begin{bmatrix}2 & 34\\36 & 2\end{bmatrix} * \begin{bmatrix}26\\13\end{bmatrix} = \begin{bmatrix}494\\962\end{bmatrix} => \begin{bmatrix}494\\962\end{bmatrix}(mod\ 37) = \begin{bmatrix}13\\0\end{bmatrix} = \begin{bmatrix}М\\А\end{bmatrix}$$

$$\begin{bmatrix}2 & 34\\36 & 2\end{bmatrix} * \begin{bmatrix}2\\0\end{bmatrix} = \begin{bmatrix}4\\72\end{bmatrix} => \begin{bmatrix}4\\72\end{bmatrix}(mod\ 37) = \begin{bmatrix}4\\35\end{bmatrix} = \begin{bmatrix}Д\\!\end{bmatrix}$$

$$\begin{bmatrix}2 & 34\\36 & 2\end{bmatrix} * \begin{bmatrix}16\\32\end{bmatrix} = \begin{bmatrix}1120\\640\end{bmatrix} => \begin{bmatrix}1120\\640\end{bmatrix}(mod\ 37) = \begin{bmatrix}10\\11\end{bmatrix} = \begin{bmatrix}Й\\К\end{bmatrix}$$

$$\begin{bmatrix}2 & 34\\36 & 2\end{bmatrix} * \begin{bmatrix}17\\9\end{bmatrix} = \begin{bmatrix}340\\630\end{bmatrix} => \begin{bmatrix}340\\630\end{bmatrix}(mod\ 37) = \begin{bmatrix}7\\1\end{bmatrix} = \begin{bmatrix}Ж\\Б\end{bmatrix}$$

Мы получили: х лммад!йкжб

6. Матрица-ключ 3x3

1) **Выбор матрицы ключа:**

$$К = \begin{bmatrix}1 & 1 & 1\\1 & 1 & 2\\1 & 2 & 3\end{bmatrix}$$

$$Det(К) = 3 + 2 + 2 - 1 - 4 - 3 = -1$$

$$К^{-1} = \begin{bmatrix}1 & 1 & -1\\1 & -2 & 1\\-1 & 1 & 0\end{bmatrix}(mod\ 37)$$

2) Кодирование матрицей 3x3

$$\begin{bmatrix}1 & 1 & -1\\1 & -2 & 1\\-1 & 1 & 0\end{bmatrix}\begin{bmatrix}18\\0\\12\end{bmatrix} = \begin{bmatrix}6\\30\\-18\end{bmatrix}(mod\ 37) = \begin{bmatrix}6\\30\\19\end{bmatrix} = \begin{bmatrix}Ё\\Э\\Т\end{bmatrix}$$

$$\begin{bmatrix}1 & 1 & -1\\1 & -2 & 1\\-1 & 1 & 0\end{bmatrix}\begin{bmatrix}0\\13\\0\end{bmatrix} = \begin{bmatrix}13\\-26\\13\end{bmatrix}(mod\ 37) = \begin{bmatrix}13\\11\\13\end{bmatrix} = \begin{bmatrix}М\\К\\М\end{bmatrix}$$

$$\begin{bmatrix}1 & 1 & -1\\1 & -2 & 1\\-1 & 1 & 0\end{bmatrix}\begin{bmatrix}12\\5\\10\end{bmatrix} = \begin{bmatrix}7\\12\\-7\end{bmatrix}(mod\ 37) = \begin{bmatrix}7\\12\\30\end{bmatrix} = \begin{bmatrix}Ж\\Л\\Э\end{bmatrix}$$

$$\begin{bmatrix}1 & 1 & -1\\1 & -2 & 1\\-1 & 1 & 0\end{bmatrix}\begin{bmatrix}11\\20\\13\end{bmatrix} = \begin{bmatrix}18\\-16\\9\end{bmatrix}(mod\ 37) = \begin{bmatrix}18\\21\\9\end{bmatrix} = \begin{bmatrix}С\\Ф\\И\end{bmatrix}$$

На выходе мы получаем закодированное сообщение:

ёэтмкмжлэсфи

3) «Вредоносное вмешательство» и расшифровка

Заменяем 3 символа в получившемся шифре:

аэтлкмжлвсфи = 0, 30, 19, 12, 11, 13, 7, 11, 2, 18, 21, 9

$$К^{-1} = \begin{bmatrix} 1 & 1 & -1 \\ 1 & -2 & 1 \\ -1 & 1 & 0 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 1 & 1 & 36 \\ 1 & 35 & 1 \\ 36 & 1 & 0 \end{bmatrix}$$

Дешифруем:

$$\begin{bmatrix} 1 & 1 & 36 \\ 1 & 35 & 1 \\ 36 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 30 \\ 19 \end{bmatrix} = \begin{bmatrix} 714 \\ 1069 \\ 30 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 26 \\ 33 \\ 30 \end{bmatrix} = \begin{bmatrix} Щ \\ \\ Э \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 36 \\ 1 & 35 & 1 \\ 36 & 1 & 0 \end{bmatrix} \begin{bmatrix} 12 \\ 11 \\ 13 \end{bmatrix} = \begin{bmatrix} 491 \\ 410 \\ 443 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 16 \\ 3 \\ 36 \end{bmatrix} = \begin{bmatrix} П \\ Г \\ ? \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 36 \\ 1 & 35 & 1 \\ 36 & 1 & 0 \end{bmatrix} \begin{bmatrix} 7 \\ 11 \\ 2 \end{bmatrix} = \begin{bmatrix} 90 \\ 394 \\ 263 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 16 \\ 24 \\ 4 \end{bmatrix} = \begin{bmatrix} П \\ Ч \\ Д \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 36 \\ 1 & 35 & 1 \\ 36 & 1 & 0 \end{bmatrix} \begin{bmatrix} 18 \\ 21 \\ 9 \end{bmatrix} = \begin{bmatrix} 363 \\ 762 \\ 669 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 30 \\ 22 \\ 3 \end{bmatrix} = \begin{bmatrix} Э \\ Ч \\ Г \end{bmatrix}$$

Мы получили: щ эпг?пчдэчг

7. Матрица-ключ 4x4

1) Выбор матрицы ключа:

$$К = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \\ 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \end{bmatrix}$$

Det(K) = $-1 - 0 - 1 - (-1) = -1$ (минорами)

$$К^{-1} = \begin{bmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & -2 & 1 \\ 1 & -2 & 1 & 0 \\ -1 & 1 & 0 & 0 \end{bmatrix} (mod\ 37) = \begin{bmatrix} 1 & 0 & 1 & 36 \\ 0 & 1 & 35 & 1 \\ 1 & 35 & 1 & 0 \\ 36 & 1 & 0 & 0 \end{bmatrix}$$

2) Кодирование матрицей 4x4

$$\begin{bmatrix}1&1&1&1\\1&1&1&2\\1&1&2&3\\1&2&3&4\end{bmatrix}\begin{bmatrix}18\\0\\12\\0\end{bmatrix}=\begin{bmatrix}30\\30\\42\\54\end{bmatrix}(mod\ 37)=\begin{bmatrix}30\\30\\5\\17\end{bmatrix}=\begin{bmatrix}Э\\Э\\Е\\Р\end{bmatrix}$$

$$\begin{bmatrix}1&1&1&1\\1&1&1&2\\1&1&2&3\\1&2&3&4\end{bmatrix}\begin{bmatrix}13\\0\\12\\5\end{bmatrix}=\begin{bmatrix}30\\35\\52\\69\end{bmatrix}(mod\ 37)=\begin{bmatrix}30\\35\\15\\32\end{bmatrix}=\begin{bmatrix}Э\\!\\О\\Я\end{bmatrix}$$

$$\begin{bmatrix}1&1&1&1\\1&1&1&2\\1&1&2&3\\1&2&3&4\end{bmatrix}\begin{bmatrix}10\\11\\20\\13\end{bmatrix}=\begin{bmatrix}54\\67\\100\\144\end{bmatrix}(mod\ 37)=\begin{bmatrix}17\\30\\26\\33\end{bmatrix}=\begin{bmatrix}Р\\Э\\Щ\\\end{bmatrix}$$

На выходе мы получаем закодированное сообщение:

ээерэ!оярэщ

3) «Вредоносное вмешательство» и расшифровка

Заменяем 3 символа в получившемся шифре:

ээжтэ!оярэщ = 30, 8, 7, 19, 30, 35, 15, 32, 17, 30, 26, 33

Дешифруем:

$$\begin{bmatrix}1&0&1&36\\0&1&35&1\\1&35&1&0\\36&1&0&0\end{bmatrix}\begin{bmatrix}30\\8\\7\\19\end{bmatrix}=\begin{bmatrix}721\\272\\317\\1088\end{bmatrix}(mod\ 37)=\begin{bmatrix}19\\13\\14\\15\end{bmatrix}=\begin{bmatrix}Ы\\М\\Ф\\М\end{bmatrix}$$

$$\begin{bmatrix}1&0&1&36\\0&1&35&1\\1&35&1&0\\36&1&0&0\end{bmatrix}\begin{bmatrix}30\\35\\15\\32\end{bmatrix}=\begin{bmatrix}1179\\592\\1270\\1115\end{bmatrix}(mod\ 37)=\begin{bmatrix}32\\0\\12\\5\end{bmatrix}=\begin{bmatrix}Я\\А\\Л\\Е\end{bmatrix}$$

$$\begin{bmatrix}1&0&1&36\\0&1&35&1\\1&35&1&0\\36&1&0&0\end{bmatrix}\begin{bmatrix}17\\30\\26\\33\end{bmatrix}=\begin{bmatrix}1231\\973\\1093\\642\end{bmatrix}(mod\ 37)=\begin{bmatrix}10\\11\\20\\13\end{bmatrix}=\begin{bmatrix}Й\\К\\У\\М\end{bmatrix}$$

Мы получили: ымфмяалейкум

Задание 2. Взлом шифра Хилла.

1. Первое зашифрованное сообщением:

б	й	.	ё	и	я	г	и	р	с	ё	ь
1	10	34	6	9	32	3	9	17	18	6	29

Второе зашифрованное сообщение:

в	х	д	и	ц	!	д	д	н	ь	ф	ш
2	22	4	9	23	35	4	4	14	29	21	25

Расшифровка первого сообщения:

и	т	м	о	space	с	п	о	р	т	?	!
9	19	13	15	33	18	16	15	17	19	36	35

2. Для того, чтобы расшифровать второе сообщение, необходимо вычислить матрицу ключа, которая определяется формулой: $K^{-1} = P \cdot C^{-1}$, где К – матрица ключа, Р – матрица, содержащая первые 4 буквы первого сообщения, С – матрица, содержащая первые 4 буквы первого закодированного сообщения.

$$\mathrm{P} = \begin{bmatrix} 9 & 13 \\ 19 & 15 \end{bmatrix};\ \mathrm{C} = \begin{bmatrix} 1 & 34 \\ 10 & 6 \end{bmatrix}$$

3. Вычисляем обратную матрицу:

$$\det \mathrm{C} = (1 * 6) - (10 * 34) = -334(mod37) = 36$$

$x * \det \mathrm{C} = 1 (\mathrm{mod}\ 37) \rightarrow x = 36$

$$\mathrm{C}^{-1} = 36 \cdot \begin{bmatrix} 6 & -34 \\ -10 & 1 \end{bmatrix} = \begin{bmatrix} 216 & -1224 \\ -360 & 36 \end{bmatrix} (\mathrm{mod}37) = \begin{bmatrix} 31 & 34 \\ 10 & 36 \end{bmatrix}$$

Для того, чтобы матрица была обратной, должно выполняться условие:

$\mathrm{C}^{-1} * \mathrm{C} = \mathrm{E}$, где Е – единичная матрица

$$\mathrm{C}^{-1} * \mathrm{C} = \begin{bmatrix} 31 & 34 \\ 10 & 36 \end{bmatrix} \cdot \begin{bmatrix} 1 & 34 \\ 10 & 6 \end{bmatrix} = \begin{bmatrix} 371 & 1258 \\ 370 & 556 \end{bmatrix} (\mathrm{mod}37) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

4. $$K^{-1} = \begin{bmatrix} 9 & 13 \\ 19 & 15 \end{bmatrix} \cdot \begin{bmatrix} 31 & 34 \\ 10 & 36 \end{bmatrix} = \begin{bmatrix} 409 & 774 \\ 739 & 1186 \end{bmatrix} (\mathrm{mod}37) = \begin{bmatrix} 2 & 34 \\ 36 & 2 \end{bmatrix}$$

5. Мы нашли матрицу ключа, теперь мы можем декодировать второе сообщение:

$$\begin{bmatrix} 2 & 34 \\ 36 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 22 \end{bmatrix} = \begin{bmatrix} 752 \\ 116 \end{bmatrix} (\mathrm{mod}37) = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} Л \\ \mathrm{E} \end{bmatrix}$$

$$\begin{bmatrix} 2 & 34 \\ 36 & 2 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 9 \end{bmatrix} = \begin{bmatrix} 314 \\ 162 \end{bmatrix} (\mathrm{mod}37) = \begin{bmatrix} 18 \\ 14 \end{bmatrix} = \begin{bmatrix} \mathrm{C} \\ \mathrm{H} \end{bmatrix}$$

$$\begin{bmatrix} 2 & 34 \\ 36 & 2 \end{bmatrix} \cdot \begin{bmatrix} 23 \\ 35 \end{bmatrix} = \begin{bmatrix} 1236 \\ 898 \end{bmatrix} (\text{mod} 37) = \begin{bmatrix} 15 \\ 10 \end{bmatrix} = \begin{bmatrix} О \\ Й \end{bmatrix}$$

$$\begin{bmatrix} 2 & 34 \\ 36 & 2 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 144 \\ 152 \end{bmatrix} (\text{mod} 37) = \begin{bmatrix} 33 \\ 4 \end{bmatrix} = \begin{bmatrix} space \\ Д \end{bmatrix}$$

$$\begin{bmatrix} 2 & 34 \\ 36 & 2 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 29 \end{bmatrix} = \begin{bmatrix} 1014 \\ 562 \end{bmatrix} (\text{mod} 37) = \begin{bmatrix} 15 \\ 7 \end{bmatrix} = \begin{bmatrix} О \\ Ж \end{bmatrix}$$

$$\begin{bmatrix} 2 & 34 \\ 36 & 2 \end{bmatrix} \cdot \begin{bmatrix} 21 \\ 25 \end{bmatrix} = \begin{bmatrix} 892 \\ 806 \end{bmatrix} (\text{mod} 37) = \begin{bmatrix} 4 \\ 29 \end{bmatrix} = \begin{bmatrix} Д \\ Ь \end{bmatrix}$$

Таким образом, мы получили исходное сообщение: ЛЕСНОЙ ДОЖДЬ

Задание 3.

А - 00000 З - 01000 П - 10000

Б - 00001 И - 01001 Р - 10001

В - 00010 Й - 01010 С - 10010

Г - 00011 К - 01011 Т - 10011

Д - 00100 Л - 01100 У - 10100

Е - 00101 М - 01101 Ф - 10101

Ё - 00110 Н - 01110 Х - 10110

Ж - 00111 О - 01111 Ц - 10111

Ч - 11000 П - 10000 Ш - 11000

Щ - 11001 Э - 11101

Ы - 11010 Ю - 11110

Ь - 11011 Я - 11111

Слово: БОКС

100001 01111 01011 100110

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} G^T = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Закодируем слово с помощью матрицы

$$G^T * \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} (\text{после } mod\ 2)$$

Следовательно, закодированное слово- 0000001001110100100011001

Случай I только 1 плохой бит, допустим изменим только 3 место

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ \mathbf{1} & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} =$$

$>$ делаем проверку на ошибочность места, которох мы заменили

$$H * \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ (после } mod\ 2)$$

Таким образом получаем $011_2 = 3$, что означает что ошибка у нас на 3 –м месте

Заменим на верное и декодируем:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \text{ (после } mod\ 2\ )$$

Эта матрица дает нам сообщение БОКС

Случай II только 2 плохих бита, допустим изменим только 17 и 22 место

$$\begin{bmatrix} 0 & 1 & 1 & \mathbf{1} & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & \mathbf{1} & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} =$$

$>$ делаем проверку на ошибочность места, которое мы заменили

$$H * \begin{bmatrix} 0 & 1 & 1 & \mathbf{1} & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & \mathbf{1} & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \text{ (после } mod\ 2)$$

Получаем что неисправными битами являются 17 и 22 биты.
Мы успешно нашли неисправные биты и сможем декодировать слово БОКС

Случай III только 3 плохих бита, допустим изменим только 17, 28 и 33 место

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & \mathbf{1} & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & \mathbf{0} \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \mathbf{1} & 0 \end{bmatrix} =>$$

делаем проверку на ошибочность места, которых мы заменили

$$H * \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & \mathbf{1} & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & \mathbf{0} \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \mathbf{1} & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & \mathbf{1} & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & \mathbf{0} \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & \mathbf{1} & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{ (после } mod\ 2)$$

Получаем что неисправными битами являются 17, 28 и 33 биты.
Мы успешно нашли неисправные биты и сможем декодировать слово БОКС

Случай IV только 4 плохих бита, допустим изменим только 7,8, 20, 25 место

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix} =$$

> делаем проверку на ошибочность места, которых мы заменили

$$H * \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{bmatrix} (\text{после } mod\ 2)$$

Получаем что неисправными битами являются 7, 8, 20 и 25 биты.
Мы успешно нашли неисправные биты и сможем декодировать слово БОКС

Вывод

В ходе выполнения задания номер один мы освоили кодирование шифром Хилла. Мы отработали навыки шифрования с использованием матриц различного размера и освоили метод нахождения обратной матрицы с помощью остатков от деления. Это позволило провести расшифровку закодированного, но испорченного сообщения, где произошло искажение нескольких символов. Мы также обнаружили, что наибольшей деформации подвержены сообщения, кодированные матрицами большего размера.

Помимо этого, мы изучили работу кода Хэмминга (7,4), который защищает от вредоносных вмешательств. На практике выяснилось, что данный метод кодирования эффективно исправляет ошибки, возникшие из-за одного "сломанного" бита в блоке, но не справляется при многократных ошибках в одном блоке.

Что касается построения матриц для кодирования и декодирования, мы изучили, как порождающая матрица G строится на основе проверочной матрицы. В матрице H располагается единичная подматрица и перестановки единиц, отвечающие за информационные и проверочные биты. Матрица G формируется путем объединения единичной матрицы и транспонированной подматрицы перестановок из матрицы H. При умножении матрицы H на транспонированную матрицу G^T результатом будет нулевая матрица, что обеспечивает контроль целостности данных. Таким образом, при корректировке матрицы H необходимо менять и матрицу G, чтобы сохранить кодовую целостность.

Данное задание дало возможность понять принципы работы как шифра Хилла, так и кода Хэмминга, а также их применение в защите информации от ошибок и искажений.