Министерство образования и науки Российской Федерации Федеральное государственное автономное образовательное учреждение высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

Факультет: Системы управления и робототехники

Отчет по лабораторной работе №1 «Кодирование и шифрование»

Преподаватель:

Перегудин А. А.,

Ассистент фак. СУиР

Выполнили:

студентка гр. R3135

Нгуен Кхань Нгок

Санкт-Петербург 2023

Содержание

Теорема Шифра Хилла

I. Шифр Хилла

- Шифр Хилла — полиграммный шифр подстановки, основанный на линейной алгебре и модульной арифметике.
- Изобретен Лестером С. Хиллом в 1929 году.
- Первый шифр замены более чем трех символов открытого текста.
- Направление алгоритма состоит в том, чтобы взять m линейных комбинаций (на кольце Z_n) из m буквенных символов plaintext, преобразуя тем самым в m буквенных символов зашифрованного сообщения (ciphertext).
- Процесс преобразования plaintext в ciphertext называется шифрованием.
- Наоборот, процесс преобразования plaintext в ciphertext называется расшифровкой
- Ключ K будет задан n-обратимой квадратной матрицей. K = $\begin{pmatrix} k_{1,1} & \cdots & k_{1,m} \\ \vdots & \ddots & \vdots \\ k_{m,1} & \cdots & k_{m,m} \end{pmatrix}$
- Необходимым и достаточным уисловием обратимости квадратной матрицы является то, что det(K) ≠ 0, тогда обратная матрица K равна: $K^{-1} = \frac{1}{\det(K)} C_k$ (где C — матрица, сопряженная с K)
- Ключ K — это набор обратимых квадратных ключевых матриц порядка n на кольце Z_n, когда определителем матрицы K будут взаимно простые числа с n, или, другими словами, det(K) ≠ 0 и НОД(det(K),n) = 1.

II. Шаги по зашифрованию и расшифрованию

a. Зашифрование информации:

Сначала нам нужно создать алфавит с количеством букв n

Нужна ключевая матрица K (обратимая квадратная матрица размера n × n), такая, что определитель матрицы и n взаимно просты).

Затем преобразуйте сообщение в ряд цифр, чтобы каждая буква представляла собой число, основанное на таблице алфавитов (нумерация от 0 до n-1).

Пример:

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

Затем мы делим последовательность на группы по m чисел и формируем матрицы сообщений с именем $A_{1\times m \text{ или } m\times 1}$ такие, что $\begin{cases} P_{1\times m} = \mathrm{A}_{1\times m} \cdot K_m \bmod n \\ \text{или} \\ P_{m\times 1} = K_m \cdot \mathrm{A}_{1\times m} \bmod n \end{cases}$ (где C: матрица зашифрования)

Заменив каждое только что найденное число в матрице C буквами алфавита, мы получим зашифрованное сообщение.

b. Расшифрованию

- Для расшифрования воспользуемся формулой: $\begin{cases} D_{1\times m} = {K^{-1}}_m \cdot P_{1\times m} \bmod n \\ \text{или} \\ D_{m\times 1} = {K^{-1}}_m \cdot P_{m\times 1} \bmod n \end{cases}$ (где D: матрица расшифрования)

Hamming(7,4)

- Код Хэмминга — это линейный код, исправляющий ошибки, названный в честь его изобретателя. Коды Хэмминга могут обнаруживать одиночные и двухбитовые ошибки и использовать синдром для проверки и исправления ошибок.
- Предположим, с кодом H(7,4)

  Вместо отправки 4-битного кода код Хэмминга (7,4) помогает нам отправить 7-битный код, включая начальные 4 бита и 3 избыточных бита, которые обнаруживают и исправляют ошибки (1 бит) во время процесса. (если есть).

Формулы и символы, используемые в кодах Хэмминга

k : message length (example: k = 4)

n: codework length (ex: 1011ccc0010ccc1110ccc → n = 7) → (7,4) code

R_c: $Coderate\ R_c = \frac{k}{n}$ (чем выше, тем лучше; более эффективным)

n = $2^p - 1 \rightarrow codework\ bits$

k = $n - p \rightarrow message\ bits$

$R_c = \frac{k}{n} = \frac{n-p}{2^p-1} = \frac{2^p-1-p}{2^p-1} = 1 - \frac{p}{2^p-1} \rightarrow code\ rate\ R_c \rightarrow 1\ as\ p \uparrow (ideal\ code\ rate)$

$M = (m_1, m_2, \dots m_k)_{1\times k} \rightarrow messsage\ vector$

$A = \left(p_1, p_2, \dots p_q\right)_{1\times q} \rightarrow check\ bit\ vector$

$G_{k\times n} = (I_k|A)_{k\times n} \rightarrow generator\ matrix$ (где I единичная матрица, $P_{d\times p} - parity$ матрица)

$H_{(n-k)\times n} = (-A^T|I_{n-k})_{(n-k)\times n} \rightarrow parity - check\ matrix$

- проверочная матрица H линейного кода C является $generator$ матрицей двойственного кода $C^{\perp}$, такой что кой что $Hc^T = \mathbf{0}$

Задачи

Задание 1: Шифр Хилла

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

- n = 33

- Ценное сообщение из 12 символов: **линейнаяалгб**
- Ключенные матрицы:

$$K_{2\times2} = \begin{bmatrix} 6 & 1 \\ 5 & 1 \end{bmatrix}, \quad K_{3\times3} = \begin{bmatrix} 3 & 5 & 7 \\ 2 & 10 & 2 \\ 1 & 5 & 3 \end{bmatrix}, \quad K_{4\times4} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 5 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

- $\det(K_2) = 6 \cdot 1 - 1 \cdot 5 = 1 \neq 0$ => НОД (1,33) = 1

- $\det(K_3) = 3 \cdot 10 \cdot 3 + 5 \cdot 2 \cdot 1 + 7 \cdot 5 \cdot 2 - 7 \cdot 10 \cdot 1 - 5 \cdot 2 \cdot 3 - 3 \cdot 5 \cdot 2 = 40 \neq 0$ => НОД (33,40) = 1

- $\det(K_4) = 1 \cdot \begin{vmatrix} 2 & 5 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{vmatrix} - 2 \cdot \begin{vmatrix} 1 & 5 & 1 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{vmatrix} + 3 \cdot \begin{vmatrix} 1 & 2 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 2 \end{vmatrix} - 4 \cdot \begin{vmatrix} 1 & 2 & 5 \\ 1 & 1 & 2 \\ 0 & 0 & 1 \end{vmatrix} =$

$$= (2 \cdot 2 \cdot 2 + 1 - 5 \cdot 1 \cdot 2 - 2) - 2(1 \cdot 2 \cdot 2 + 1 - 5 \cdot 1 \cdot 2 - 1) + 3(2 - 2 \cdot 1 \cdot 2) - 4(1 - 2)$$
$$= -3 + 12 - 6 + 4 = 7 \neq 0$$

=> НОД (7,33) = 1

У нас сообщение: линейнаяалгб

=>

л	и	н	е	й	н	а	я	а	л	г	б
12	9	14	5	10	14	0	32	0	12	3	1

а. Зашифруем сообщение с помощью каждого из ключей, используя метод шифрования Хилла

Формула зашифрования : $\begin{cases} E_{1\times m} = \mathrm{A}_{1\times m} \cdot K_m \ mod\ n \\ \text{или} \\ E_{m\times 1} = K_m \cdot \mathrm{A}_{m\times 1} \ mod\ n \end{cases}$

- Для $\mathbf{K_2}$:

- (л и) → $(12 \quad 9)\begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} = (12 \times 6 + 9 \times 5 \quad 12 \times 1 + 9 \times 1) = (117 \quad 21) \equiv (18 \quad 21)\ mod\ 33$
- (н е) → $(14 \quad 5)\begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} = (14 \times 6 + 5 \times 5 \quad 14 \times 1 + 5 \times 1) = (109 \quad 19) \equiv (10 \quad 19) \bmod 33$
- (й н) → $(10 \quad 14)\begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} = (10 \times 6 + 14 \times 5 \quad 10 \times 1 + 14 \times 1) = (130 \quad 24) \equiv (31 \quad 24) \bmod 33$
- (а я) → $(0 \quad 32)\begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} = (0 \times 6 + 32 \times 5 \quad 0 \times 1 + 32 \times 1) = (160 \quad 32) \equiv (28 \quad 32) \bmod 33$
- (а л) → $(0 \quad 12)\begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} = (0 \times 6 + 12 \times 5 \quad 0 \times 1 + 12 \times 1) = (60 \quad 12) \equiv (27 \quad 12) \bmod 33$
- (г б) → $(3 \quad 1)\begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} = (3 \times 6 + 1 \times 5 \quad 3 \times 1 + 1 \times 1) = (23 \quad 4) \equiv (23 \quad 4) \bmod (33)$

12	9	14	5	10	14	0	32	0	12	3	1	→	18	21	10	19	31	24	28	32	27	12	23	4
л	и	н	е	й	н	а	я	а	л	г	б		с	ф	й	т	ю	ч	ы	я	ъ	л	ц	д

линейнаяалгб → сфйтючыяълцд

12 9 14 5 10 14 0 32 0 12 3 1 → 18 21 10 19 31 24 28 32 12 23 4

- Для $\boldsymbol{K_3}$:
  - (л и н) → $(12\ \ 9\ \ 14)\begin{pmatrix}3 & 5 & 7\\ 2 & 10 & 2\\ 1 & 5 & 3\end{pmatrix} = (68\ \ 220\ \ 144) \equiv (2\ \ 22\ \ 12)\ mod\ 33$
  - (е й н) → $(5\ \ 10\ \ 14)\begin{pmatrix}3 & 5 & 7\\ 2 & 10 & 2\\ 1 & 5 & 3\end{pmatrix} = (49\ \ 195\ \ 97) \equiv (16\ \ 30\ \ 31)\ mod\ 33$
  - (а я а) → $(0\ \ 32\ \ 0)\begin{pmatrix}3 & 5 & 7\\ 2 & 10 & 2\\ 1 & 5 & 3\end{pmatrix} = (64\ \ 320\ \ 64) \equiv (31\ \ 23\ \ 31)\ mod\ 33$
  - (л г б) → $(12\ \ 3\ \ 1)\begin{pmatrix}3 & 5 & 7\\ 2 & 10 & 2\\ 1 & 5 & 3\end{pmatrix} = (43\ \ 95\ \ 93) \equiv (10\ \ 29\ \ 27)\ mod\ 33$

12	9	14	5	10	14	0	32	0	12	3	1	→	2	22	12	16	30	31	31	23	31	10	29	27
л	и	н	е	й	н	а	я	а	л	г	б		с	ф	й	т	ю	ч	ы	я	ъ	л	ц	д

линейнаяалгб → вчлпэююцюйьъ

12 9 14 5 10 14 0 32 0 12 3 1 → 2 22 12 16 30 31 31 23 31 10 29 27

- Для $\boldsymbol{K_4}$:
  - (л и н е) → $(12\ \ 9\ \ 14\ \ 5)\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 5 & 1\\ 1 & 1 & 2 & 1\\ 0 & 0 & 1 & 2\end{pmatrix} = (35\ \ 56\ \ 114\ \ 81) \equiv (2\ \ 23\ \ 15\ \ 15)\ mod\ 33$
  - (й н а я) → $(10\ \ 14\ \ 0\ \ 32)\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 5 & 1\\ 1 & 1 & 2 & 1\\ 0 & 0 & 1 & 2\end{pmatrix} = (24\ \ 18\ \ 132\ \ 118) \equiv (24\ \ 15\ \ 0\ \ 19)\ mod\ 33$
  - (а л г б) → $(0\ \ 12\ \ 3\ \ 1)\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 5 & 1\\ 1 & 1 & 2 & 1\\ 0 & 0 & 1 & 2\end{pmatrix} = (15\ \ 27\ \ 67\ \ 17) \equiv (15\ \ 27\ \ 1\ \ 17)\ mod\ 33$

12	9	14	5	10	14	0	32	0	12	3	1	→	2	23	15	15	24	15	0	19	15	27	1	17
л	и	н	е	й	н	а	я	а	л	г	б		в	ц	о	о	ч	о	а	т	о	ъ	б	р

⇨ **линейнаяалгб → вцоочоатоъбр**

12 9 14 5 10 14 0 32 0 12 3 1 → 2 23 15 15 24 15 0 19 15 27 1 17

b. Заменим в каждом из них по три символа на какие-то другие (случайные) символы

1. сфйтючыяълцд → сфйтючлуклцд - 18 21 10 19 31 24 12 20 11 12 23 49
2. вчлпэююцюйьъ → вагаэююцюйьъ - 2 0 3 0 30 31 31 23 31 10 29 27
3. вцоочоатоъбр → вцнетоатоъбр - 2 23 14 5 19 15 0 19 15 27 1 17

c. Расшифруйте каждое из получившихся сообщений, используя обратные матрицы от матриц-ключей

Формула: $\begin{cases}P_{1\times m} = \cdot E_{1\times m}\ \cdot {K^{-1}}_m\ mod\ n\\ \text{или}\\ P_{m\times 1} = {K^{-1}}_m \cdot E_{m\times 1}\ mod\ n\end{cases}$, $K^{-1} = \frac{1}{\det(K)} C^T = \det(K)^{-1} \times C^T\ mod\ 33$

- Для $\mathbf{K_2}$:

1. Сфйтючыяълцд - 18 21 10 19 31 24 28 32 12 23 4

$$K_2 = \begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix} \rightarrow K^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 6 & 1 \\ 5 & 1 \end{pmatrix}^{-1} = (6 \times 1 - 1 \times 5)^{-1} \begin{pmatrix} 1 & -1 \\ -5 & 6 \end{pmatrix}$$

$$\leftrightarrow \begin{pmatrix} 1 & -1 \\ -5 & 6 \end{pmatrix} \equiv \begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} mod\ 33$$

- $(18 \quad 21)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (18 \times 1 + 21 \times 28 \quad 18 \times 32 + 21 \times 6) = (606 \quad 702) \equiv (12 \quad 9)\ mod\ 33$
- $(10 \quad 19)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (10 \times 1 + 19 \times 28 \quad 10 \times 32 + 19 \times 6) = (542 \quad 434) \equiv (14 \quad 5)\ mod\ 33$
- $(31 \quad 24)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (31 \times 1 + 24 \times 28 \quad 31 \times 32 + 24 \times 6) = (703 \quad 1136) \equiv (10 \quad 14)\ mod\ 33$
- $(28 \quad 32)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (28 \times 1 + 32 \times 28 \quad 28 \times 32 + 32 \times 6) = (924 \quad 1088) \equiv (0 \quad 32)\ mod\ 33$
- $(27 \quad 12)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (27 \times 1 + 12 \times 28 \quad 27 \times 32 + 12 \times 6) = (363 \quad 936) \equiv (0 \quad 12)\ mod\ 33$
- $(23 \quad 4)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (23 \times 1 + 4 \times 28 \quad 23 \times 32 + 4 \times 6) = (135 \quad 760) \equiv (3 \quad 1)\ mod\ 33$

18	21	10	19	31	24	28	32	27	12	23	4	→	12	9	14	5	10	14	0	32	0	12	3	1
с	ф	й	т	ю	ч	ы	я	ъ	л	ц	д		л	и	н	е	й	н	а	я	а	л	г	б

сфйтючыяълцд → линейнаяалгб
18 21 10 19 31 24 28 32 27 12 23 4 → 12 9 14 5 10 14 0 32 0 12 3 1

2. сфйтючыяълцд → сфйтючлуклцд - 18 21 10 19 31 24 12 20 11 12 23 4

- $(18 \quad 21)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (18 \times 1 + 21 \times 28 \quad 18 \times 32 + 21 \times 6) = (606 \quad 702) \equiv (12 \quad 9)\ mod\ 33$
- $(10 \quad 19)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (10 \times 1 + 19 \times 28 \quad 10 \times 32 + 19 \times 6) = (542 \quad 434) \equiv (14 \quad 5)\ mod\ 33$
- $(31 \quad 24)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (31 \times 1 + 24 \times 28 \quad 31 \times 32 + 24 \times 6) = (703 \quad 1136) \equiv (10 \quad 14)\ mod\ 33$
- $(12 \quad 20)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (28 \times 1 + 32 \times 28 \quad 28 \times 32 + 32 \times 6) = (572 \quad 504) \equiv (11 \quad 9)\ mod\ 33$
- $(11 \quad 12)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (27 \times 1 + 12 \times 28 \quad 27 \times 32 + 12 \times 6) = (347 \quad 424) \equiv (17 \quad 28)\ mod\ 33$
- $(23 \quad 4)\begin{pmatrix} 1 & 32 \\ 28 & 6 \end{pmatrix} = (23 \times 1 + 4 \times 28 \quad 23 \times 32 + 4 \times 6) = (135 \quad 760) \equiv (3 \quad 1)\ mod\ 33$

18	21	10	19	31	24	12	20	11	12	23	4	→	12	9	14	5	10	14	11	9	17	28	3	1
с	ф	й	т	ю	ч	л	у	к	л	ц	д		л	и	н	е	й	н	к	и	р	ы	г	б

сфйтючлуклцд→ линейнкирыгб
18 21 10 19 31 24 12 20 11 12 23 4 → 12 9 14 5 10 14 11 9 17 28 3 1

- Для $\mathbf{K_3}$:

$$K_3 = \begin{pmatrix} 3 & 5 & 7 \\ 2 & 10 & 2 \\ 1 & 5 & 3 \end{pmatrix}$$

1. $K_3^{-1} = \det(K_3)^{-1} \times C_3^{T}$
2. $C_K^{T} = \begin{pmatrix} 3 & 5 & 7 \\ 2 & 10 & 2 \\ 1 & 5 & 3 \end{pmatrix}^T = \begin{pmatrix} 20 & -4 & 0 \\ 20 & 2 & -10 \\ -60 & 8 & 20 \end{pmatrix}^T = \begin{pmatrix} 20 & 20 & -60 \\ -4 & 2 & 8 \\ 0 & -10 & 20 \end{pmatrix} \equiv \begin{pmatrix} 20 & 20 & 6 \\ 29 & 2 & 8 \\ 0 & 23 & 20 \end{pmatrix} \ mod\ 33$
3. $\det(K_3) \cdot \det(K_3)^{-1} \equiv 1\ mod\ 33 \leftrightarrow 40 \cdot \det(K_3)^{-1} \equiv 1\ mod\ 33$

$40 \cdot 40^{-1} \equiv 1\ mod\ 33$	$40 \cdot 7 \equiv 16\ mod\ 33$	$40 \cdot 14 \equiv 32\ mod\ 33$
$40 \cdot 1 \equiv 7\ mod\ 33$	$40 \cdot 8 \equiv 23\ mod\ 33$	$40 \cdot 15 \equiv 6\ mod\ 33$
$40 \cdot 2 \equiv 14\ mod\ 33$	$40 \cdot 9 \equiv 30\ mod\ 33$	$40 \cdot 16 \equiv 13\ mod\ 33$
$40 \cdot 3 \equiv 21\ mod\ 33$	$40 \cdot 10 \equiv 4\ mod\ 33$	$40 \cdot 17 \equiv 20\ mod\ 33$
$40 \cdot 4 \equiv 28\ mod\ 33$	$40 \cdot 11 \equiv 11\ mod\ 33$	$40 \cdot 18 \equiv 27\ mod\ 33$
$40 \cdot 5 \equiv 2\ mod\ 33$	$40 \cdot 12 \equiv 18\ mod\ 33$	$40 \cdot 19 \equiv 1\ mod\ 33$
$40 \cdot 6 \equiv 9\ mod\ 33$	$40 \cdot 13 \equiv 25\ mod\ 33$	$=> \mathbf{det(K_3)^{-1} = 19}$

4. $K_3^{-1} = \det(K_3)^{-1} \times C_K^{T} = 19 \times \begin{pmatrix} 20 & 20 & 6 \\ 29 & 2 & 8 \\ 0 & 23 & 20 \end{pmatrix} = \begin{pmatrix} 380 & 380 & -1140 \\ -76 & 38 & 152 \\ 0 & -190 & 380 \end{pmatrix} \equiv \begin{pmatrix} 17 & 17 & 15 \\ 23 & 5 & 20 \\ 0 & 8 & 17 \end{pmatrix} mod\ 33$

Расшифруем зашифрованное сообщение

1. **вчлпэююцюйьъ - 2 22 12 16 30 31 31 23 31 10 29 27**

- $\rightarrow (2 \quad 22 \quad 12) \begin{pmatrix} 17 & 17 & 15 \\ 23 & 5 & 20 \\ 0 & 8 & 17 \end{pmatrix} = (540 \quad 240 \quad 674) \equiv (12 \quad 9 \quad 14)\ mod\ 33$
- $(16 \quad 30 \quad 31) \begin{pmatrix} 17 & 17 & 15 \\ 23 & 5 & 20 \\ 0 & 8 & 17 \end{pmatrix} = (962 \quad 670 \quad 1367) \equiv (5 \quad 10 \quad 14)\ mod\ 33$
- $(31 \quad 23 \quad 31) \begin{pmatrix} 17 & 17 & 15 \\ 23 & 5 & 20 \\ 0 & 8 & 17 \end{pmatrix} = (1056 \quad 890 \quad 1452) \equiv (0 \quad 32 \quad 0)\ mod\ 33$
- $(10 \quad 29 \quad 27) \begin{pmatrix} 17 & 17 & 15 \\ 23 & 5 & 20 \\ 0 & 8 & 17 \end{pmatrix} = (837 \quad 531 \quad 1189) \equiv (12 \quad 3 \quad 1)\ mod\ 33$

2	22	12	16	30	31	31	23	31	10	29	27	→	12	9	14	5	10	14	0	32	0	12	3	1
в	ц	о	о	ч	о	а	т	о	ъ	б	р		л	и	н	е	й	н	а	я	а	л	г	б

вчлпэююцюйьъ → линейнаяалгб

2 22 12 16 30 31 31 23 31 10 29 27→12 9 14 5 10 14 0 32 0 12 3 1

2. вчлпэююцюйьъ → **вагаэююцюйьъ - 2 0 3 0 30 31 31 23 31 10 29 27**

- $(2 \quad 0 \quad 3)\begin{pmatrix}17 & 17 & 15\\ 23 & 5 & 20\\ 0 & 8 & 17\end{pmatrix} = (34 \quad 58 \quad 81) \equiv (1 \quad 25 \quad 15)\ mod\ 33$
- $(0 \quad 30 \quad 31)\begin{pmatrix}17 & 17 & 15\\ 23 & 5 & 20\\ 0 & 8 & 17\end{pmatrix} = (690 \quad 398 \quad 1127) \equiv (30 \quad 2 \quad 5)\ mod\ 33$
- $(31 \quad 23 \quad 31)\begin{pmatrix}17 & 17 & 15\\ 23 & 5 & 20\\ 0 & 8 & 17\end{pmatrix} = (1056 \quad 890 \quad 1452) \equiv (0 \quad 32 \quad 0)\ mod\ 33$
- $(10 \quad 29 \quad 27)\begin{pmatrix}17 & 17 & 15\\ 23 & 5 & 20\\ 0 & 8 & 17\end{pmatrix} = (837 \quad 531 \quad 1189) \equiv (12 \quad 3 \quad 1)\ mod\ 33$

2	0	3	0	30	31	31	23	31	10	29	27	→	1	25	15	30	2	5	0	32	0	12	3	1
в	ц	о	о	ч	о	а	т	о	ъ	б	р		б	ш	о	э	в	е	а	я	а	л	г	б

сфйтючлуклцд→бшоэвеаяалгб
2 0 3 0 30 31 31 23 31 10 29 27→ 1 25 15 30 2 5 0 32 0 12 3 1

- Для $\mathbf{K_4}$:

$$K_4 = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 5 & 1\\ 1 & 1 & 2 & 1\\ 0 & 0 & 1 & 2\end{pmatrix} \rightarrow {K_4}^{-1} = \det(K_4)^{-1} \times {C_4}^T$$

1. $${C_4}^T = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 5 & 1\\ 1 & 1 & 2 & 1\\ 0 & 0 & 1 & 2\end{pmatrix}^T = \begin{pmatrix}-3 & 6 & -2 & 1\\ -4 & 1 & 2 & -1\\ 14 & -7 & 0 & 0\\ 1 & -9 & 3 & -2\end{pmatrix}^T = \begin{pmatrix}-3 & -4 & 14 & 1\\ 6 & 1 & -7 & -9\\ -2 & 2 & 0 & 3\\ 1 & -1 & 0 & -2\end{pmatrix} \equiv \begin{pmatrix}30 & 29 & 14 & 1\\ 6 & 1 & 26 & 24\\ 31 & 2 & 0 & 3\\ 1 & 32 & 0 & 31\end{pmatrix} mod\ 33$$

2. $\det(K_4) = 7 \rightarrow \det(K_4) \times \det(K_4)^{-1} \equiv 1\ mod\ (33) \leftrightarrow 7 \times \det(K_4)^{-1} \equiv 1\ mod\ 33$

$7 \cdot 7^{-1} \equiv 1\ mod\ 33$	$7 \cdot 7 \equiv 16\ mod\ 33$	$7 \cdot 14 \equiv 32\ mod\ 33$
$7 \cdot 1 \equiv 7\ mod\ 33$	$7 \cdot 8 \equiv 23\ mod\ 33$	$7 \cdot 15 \equiv 6\ mod\ 33$
$7 \cdot 2 \equiv 14\ mod\ 33$	$7 \cdot 9 \equiv 30\ mod\ 33$	$7 \cdot 16 \equiv 13\ mod\ 33$
$7 \cdot 3 \equiv 21\ mod\ 33$	$7 \cdot 10 \equiv 4\ mod\ 33$	$7 \cdot 17 \equiv 20\ mod\ 33$
$7 \cdot 4 \equiv 28\ mod\ 33$	$7 \cdot 11 \equiv 11\ mod\ 33$	$7 \cdot 18 \equiv 27\ mod\ 33$
$7 \cdot 5 \equiv 2\ mod\ 33$	$7 \cdot 12 \equiv 18\ mod\ 33$	$7 \cdot 19 \equiv 1\ mod\ 33$
$7 \cdot 6 \equiv 9\ mod\ 33$	$7 \cdot 13 \equiv 25\ mod\ 33$	$=>\ \mathbf{\det(K_4)^{-1} = 19}$

3. $${K_4}^{-1} = \det(K_4)^{-1} \times {C_4}^T = 19 \times \begin{pmatrix}30 & 29 & 14 & 1\\ 6 & 1 & 26 & 24\\ 31 & 2 & 0 & 3\\ 1 & 32 & 0 & 2\end{pmatrix} = \begin{pmatrix}570 & 551 & 266 & 19\\ 114 & 19 & 494 & 456\\ 589 & 38 & 0 & 57\\ 19 & 608 & 0 & 38\end{pmatrix}$$

$$\equiv \begin{pmatrix}9 & 23 & 2 & 19\\ 15 & 19 & 32 & 27\\ 28 & 5 & 0 & 24\\ 19 & 14 & 0 & 5\end{pmatrix} mod\ 33$$

Расшифруем зашифрованное сообщение

1. вцоочоатоъбр **- 2 23 15 15 24 15 0 19 15 27 1 17**

- $(2 \quad 23 \quad 15 \quad 15)\begin{pmatrix} 9 & 23 & 2 & 19 \\ 15 & 19 & 32 & 27 \\ 28 & 5 & 0 & 24 \\ 19 & 14 & 0 & 5 \end{pmatrix} = (1068 \quad 768 \quad 740 \quad 1094) \equiv (12 \quad 9 \quad 14 \quad 5)\ mod\ 33$
- $(24 \quad 15 \quad 0 \quad 19)\begin{pmatrix} 9 & 23 & 2 & 19 \\ 15 & 19 & 32 & 27 \\ 28 & 5 & 0 & 24 \\ 19 & 14 & 0 & 5 \end{pmatrix} = (802 \quad 1130 \quad 528 \quad 956) \equiv (10 \quad 8 \quad 0 \quad 32)\ mod\ 33$
- $(15 \quad 27 \quad 1 \quad 17)\begin{pmatrix} 9 & 23 & 2 & 19 \\ 15 & 19 & 32 & 27 \\ 28 & 5 & 0 & 24 \\ 19 & 14 & 0 & 5 \end{pmatrix} = (891 \quad 1101 \quad 894 \quad 1123) \equiv (0 \quad 12 \quad 3 \quad 1)\ mod\ 33$

2	23	15	15	24	15	0	19	15	27	1	17	→	12	9	14	5	10	14	0	32	0	12	3	1
в	ц	о	о	ч	о	а	т	о	ъ	б	р		л	и	н	е	й	н	а	я	а	л	г	б

вцоочоатоъбр → линейнаяагбр

2 23 15 15 24 15 0 19 15 27 1 17 – 12 9 14 5 10 14 0 32 0 12 3 1

2. вцоочоатоъбр → **вцнетоатоъбр - 2 23 14 5 19 15 0 19 15 27 1 17**

- $(2 \quad 23 \quad 14 \quad 5)\begin{pmatrix} 9 & 23 & 2 & 19 \\ 15 & 19 & 32 & 27 \\ 28 & 5 & 0 & 24 \\ 19 & 14 & 0 & 5 \end{pmatrix} = (850 \quad 623 \quad 740 \quad 1020) \equiv (25 \quad 29 \quad 14 \quad 30)\ mod\ 33$
- $(19 \quad 15 \quad 0 \quad 19)\begin{pmatrix} 9 & 23 & 2 & 19 \\ 15 & 19 & 32 & 27 \\ 28 & 5 & 0 & 24 \\ 19 & 14 & 0 & 5 \end{pmatrix} = (757 \quad 988 \quad 518 \quad 861) \equiv (31 \quad 31 \quad 23 \quad 3)\ mod\ 33$
- $(15 \quad 27 \quad 1 \quad 17)\begin{pmatrix} 9 & 23 & 2 & 19 \\ 15 & 19 & 32 & 27 \\ 28 & 5 & 0 & 24 \\ 19 & 14 & 0 & 5 \end{pmatrix} = (891 \quad 1101 \quad 894 \quad 1123) \equiv (0 \quad 12 \quad 3 \quad 1)\ mod\ 33$

2	23	14	5	19	15	0	19	15	27	1	17	→	25	29	14	30	31	31	23	3	0	12	3	1
в	ц	н	е	т	о	а	т	о	ъ	б	р		ш	ь	н	э	ю	ю	ц	г	а	л	г	б

вцнетоатоъбр → шьнэююцгалгбр

2 23 14 5 19 15 0 19 15 27 1 17 → 25 29 14 30 31 31 23 3 0 12 3 1

Задание 2. Взлом шифра Хилла.

- Сообщение 1: Приветствиее → 16 17 9 2 5 19 18 19 2 9 5 5
- Сообщение 2: непобедимыйй → 14 5 16 15 1 5 4 9 13 28 10 10
- Ключеная матрица: $K_{2\times2}$

$$\rightarrow K_{2\times2} = \begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix}$$

П	Р	И	В	Е	Т	С	Т	В	И	Е	Е
16	17	9	2	5	19	18	19	2	9	5	5

Зашифруем зашифрованное сообщение

- (п р) → $(16 \quad 17)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (419 \quad 501) \equiv (23 \quad 6)\ mod\ 33$ → (ц ё)
- (и в) → $(9 \quad 2)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (213 \quad 244) \equiv (15 \quad 13)\ mod\ 33$ → (о м)
- (е т) → $(5 \quad 19)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (172 \quad 225) \equiv (7 \quad 27)\ mod\ 33$ → (ж ъ)
- (с т) → $(18 \quad 19)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (471 \quad 563) \equiv (9 \quad 2)\ mod\ 33$ → (и в)
- (в и) → $(2 \quad 9)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (73 \quad 97) \equiv (7 \quad 31)\ mod\ 33$ → (ж ю)
- (Е е) → $(5 \quad 5)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (130 \quad 155) \equiv (31 \quad 23)\ mod\ 33$ → (ю ц)

16179251918192955 → 2361513727927313123

Приветствиее → цёомжъивжююц

Н	Е	П	О	Б	Е	Д	И	М	Ы	Й	Й
14	5	16	15	1	5	4	9	13	28	10	10

Зашифруем зашифрованное сообщение

- (н е) → $(14 \quad 5)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (337 \quad 389) \equiv (7 \quad 26)\ mod\ 33$ → (ж щ)
- (п о) → $(16 \quad 15)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (413 \quad 491) \equiv (17 \quad 29)\ mod\ 33$ → (р ь)
- (б е) → $(1 \quad 5)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (38 \quad 51) \equiv (5 \quad 18)\ mod\ 33$ → (е с)
- (д и) → $(4 \quad 9)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (119 \quad 149) \equiv (20 \quad 17)\ mod\ 33$ → (у р)
- (м ы) → $(13 \quad 28)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (383 \quad 478) \equiv (20 \quad 16)\ mod\ 33$ → (у п)
- (й й) → $(10 \quad 10)\begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} = (260 \quad 310) \equiv (29 \quad 13)\ mod\ 33$ → (ь м)

14516151549132810 10 → 7261729518201720162913

непобедимыйй → жщрьесурупьм

Имея на руках:

- E: Приветствиее 16 17 9 2 5 19 18 19 2 9 5 5
  → P: цёомжъивжююц 23 6 15 13 7 27 9 2 7 31 31 23
- E: ?
  → P: жщрьесурупьм 7 26 17 29 5 18 20 17 20 16 29 13

Расшифруйте 2-ое зашифрованное сообщение: жщрьесурупьм **7 26 17 29 5 18 20 17 20 16 29 13**

- Найти ключная матрица K:

У нас формула: $P = E \times K \leftrightarrow K = E^{-1} \times P \leftrightarrow K^{-1} = P^{-1} \times E$

1. $E = \begin{pmatrix} 2 & 9 \\ 5 & 5 \end{pmatrix}$
2. $\det(E) = \begin{vmatrix} 2 & 9 \\ 5 & 5 \end{vmatrix} = -35 \equiv 31\ mod\ 33$
3. $\det (E)^{-1} \equiv 16\ mod\ 33$
4. $C_E^T = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 5 & -9 \\ -5 & 2 \end{pmatrix} \equiv \begin{pmatrix} 5 & 24 \\ 28 & 2 \end{pmatrix} mod\ 33$
5. $E^{-1} = 16 \begin{pmatrix} 5 & 24 \\ 28 & 2 \end{pmatrix} = \begin{pmatrix} 80 & 384 \\ 448 & 32 \end{pmatrix} \equiv \begin{pmatrix} 14 & 21 \\ 19 & 32 \end{pmatrix} mod\ 33$
6. $K = \begin{pmatrix} 14 & 21 \\ 19 & 32 \end{pmatrix} \begin{pmatrix} 7 & 31 \\ 31 & 23 \end{pmatrix} = \begin{pmatrix} 749 & 917 \\ 1125 & 1325 \end{pmatrix} \equiv \begin{pmatrix} 23 & 26 \\ 3 & 5 \end{pmatrix} mod\ 33$
7. $\det(K) = \begin{vmatrix} 23 & 26 \\ 3 & 5 \end{vmatrix} = 37 \equiv 4\ mod\ 33$
8. $\det(K) \cdot \det(K)^{-1} \equiv 1\ mod\ 33 \leftrightarrow 4 \cdot \det(K)^{-1} \equiv 1\ mod\ 33 \rightarrow \det(K)^{-1} = 25 \equiv 1\ mod\ 33$
9. $C_K^T = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 5 & -26 \\ -3 & 23 \end{pmatrix} \equiv \begin{pmatrix} 5 & 7 \\ 30 & 23 \end{pmatrix}$
10. $K^{-1} = \det(K)^{-1} \cdot C_K^T = 25 \cdot \begin{pmatrix} 5 & 7 \\ 30 & 23 \end{pmatrix} = \begin{pmatrix} 125 & 175 \\ 750 & 575 \end{pmatrix} \equiv \begin{pmatrix} 26 & 10 \\ 24 & 14 \end{pmatrix}$

Расшифруем 2-ое зашифрованное сообщение

- $(7 \quad 26) \begin{pmatrix} 26 & 10 \\ 24 & 14 \end{pmatrix} = (806 \quad 434) \equiv (14 \quad 5)\ mod\ 33 \rightarrow$ (н е)
- $(17 \quad 29) \begin{pmatrix} 26 & 10 \\ 24 & 14 \end{pmatrix} = (1138 \quad 576) \equiv (16 \quad 15)\ mod\ 33 \rightarrow$ (п о)
- $(5 \quad 18) \begin{pmatrix} 26 & 10 \\ 24 & 14 \end{pmatrix} = (562 \quad 302) \equiv (1 \quad 5)\ mod\ 33 \rightarrow$ (б е)
- $(20 \quad 17) \begin{pmatrix} 26 & 10 \\ 24 & 14 \end{pmatrix} = (928 \quad 438) \equiv (4 \quad 9)\ mod\ 33 \rightarrow$ (д и)
- $(20 \quad 16) \begin{pmatrix} 26 & 10 \\ 24 & 14 \end{pmatrix} = (904 \quad 404) \equiv (13 \quad 8)\ mod\ 33 \rightarrow$ (м ы)
- $(29 \quad 13) \begin{pmatrix} 26 & 10 \\ 24 & 14 \end{pmatrix} = (1066 \quad 472) \equiv (10 \quad 10)\ mod\ 33 \rightarrow$ (й й)

7 26 17 29 5 18 20 17 20 16 29 13 → 14 5 16 15 1 5 4 9 13 8 10 10

жщрьесурупьм → непобедимыйй

Задание 3. Код Хэмминга

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010
К	Л	М	Н	О	П	Р	С	Т	У	Ф
01011	01100	01101	01110	01111	10000	10001	10010	10011	10100	10101
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	
10110	10111	11000	11001	11010	11011	11100	11101	11110	11111	

- Интересное слово из 4 букв: **НГОК**
- Закодированное слово будет иметь следующий вид: 01110 00011 01111 01011

a. Составьте матрицы G и H

- *У нас размер данных = 5* → $k = 5$
- $2^p \geq (p + m) + 1$

$\leftrightarrow 2^p \geq p + 6 \leftrightarrow 2^4 \geq 10 \leftrightarrow 16 \geq 10 \rightarrow p = 4$

- $n = k + p = 5 + 4 = 9$

→ Имея 5 бит данных, нам нужно еще 4 бита четности → $H(9,5)$

$k \rightarrow$ *data bits*

$p \rightarrow$ *parity bits*

$2^p \geq (p + m) + 1$

Порождающую матрицу можно представить двумя подматрицами – информационной и проверочной. Информационная матрица E имеет размер (k×k), проверочная подматрица A – размер (k×p)

- Проверочная подматрица строится путем подбора различных p-разрядных комбинаций, удовлетворяющих следующим условиям:
  1. В каждой строке проверочной подматрицы должно быть не менее $d_0 - 1$ единиц.
  2. Сумма по модулю 2 двух любых строк должна иметь не менее $d_0 - 2$ единицы.
- Все биты в позициях, которые являются степенями двойки, используются как биты четности. (позиции типа 1, 2, 4, 8, 16, 32, 64 и т. д. или, другими словами, 20, 21, 22, 23, 24, 25, 26 и т. д.)
- Все остальные битовые позиции, используемые для данных, будут зашифрованы. (позиции 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17 и т.д.)
- Положение проверочного бита определяет последовательность битов, которые он поочередно проверяет и пропускает.
  - **p1 (n=1):** пропустить 0 бит (n-1), проверить 1 бит (n
  - **p2 (n=2):** пропустить 1 бит (n-1), проверить 2 бита (n)
  - **p4(n=4):** пропустить 3 бита(n-1), проверить 4 бита(n), пропустить 4 бита(n), проверить 4 бита(n), пропустить 4 бита(n) и т.д.
  - **p8(n=8):** пропустить 7 бит(n-1), проверить 8 бит(n), пропустить 8 бит(n), проверить 8 бит(n), пропустить 8 бит(n) и т.д.

position		1	2	3	4	5	6	7	8	9
encoded data bit		p1	p2	d1	p3	d2	d3	d4	p4	d5
parity bit	p1	1	0	1	0	1	0	1	0	1
	p2	0	1	1	0	0	1	1	0	0
	p3	0	0	0	1	1	1	1	0	0
	p4	0	0	0	0	0	0	0	1	1

если столбцы четности в приведенной выше таблице были удалены, мы получаем таблицу

	d1	d2	d3	d4	d5
p1	1	1	0	1	1
p2	1	0	1	1	0
p3	0	1	1	1	0
p4	0	0	0	0	1

Итак, проверочная матрица будет:

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow A^T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

тогда сходство со строками 1, 2, 4 и 8 порождающей матрицы (G) будет выражаться следующим образом

$$G = (I_k | A^T) \leftrightarrow G_{5\times 9} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$H = (A | I_{n-k}) \leftrightarrow H_{4\times 9} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

b. Ответы вопросов

1. Почему у них именно такие строки/столбцы?

- G называется порождающей матриц, используемой для создания кода длиной 9 бит, включая 4 бита проверки четности и 5 бита данных. Она обычно имеет размерность (k x n), где k - число информационных символов, а n число кодовых символов. Строки матрицы G соответствуют информационным символам, а столбцы - кодовым символам.

- Матрица H (матрица проверки четности) используется для декодирования данных и обнаружения и исправления ошибок. Она обычно имеет размерность ((n-k) x n), где (n-k) - число проверочных символов. Строки матрицы H соответствуют проверочным символам, а столбцы - кодовым символам.

2. Выбираются ли эти матрицы единственным образом, или их можно составить по разном (если да, то как)?

- Выбор матриц G и H не является единственным. Существуют различные способы выбора и построения этих матриц в соответствии с требованиями конкретного кода с исправлением ошибок. При выборе матрицы G и H необходимо учитывать такие факторы, как эффективность кодирования и декодирования, сложность реализации, свойства исправления ошибок и другие требования.

- Выбор матриц G и H основан на следующих правилах:
  1. Матрица G должна иметь столько строк, сколько битов данных и проверочных разрядов в кодированном сообщении.
  2. Матрица H должна иметь столько столбцов, сколько битов данных в кодированном сообщении.
  3. Каждая строка матрицы G должна быть линейно независимой от других строк.
  4. Каждая строка матрицы H должна быть линейно независимой от других строк.

3. Как соотносятся образ одной матрицы с ядром другой матрицы?

- Если вектор x не находится в ядро матрицы H ($x \notin \mathrm{Ker}(H)$), то образ матрицы H при умножении на x будет ненулевым вектором ($H*x \neq 0$).

- Если вектор x находится в ядре матрицы H (т.е. x ∈ Ker(H)), то изображение матрицы H при умножении на x = ненулевым вектором (H*x = 0).
- Это свойство позволяет эффективно обнаруживать и исправлять ошибки при декодировании данных с использованием H-матрицы.

c. Закодируем слово из 4 букв, представленное двоичным кодом, с помощью матрицы G

У нас слово из 4 букв, представленное двоичным кодом

НГОК → 01110 00011 01111 01011

Формула: $c = a \oplus G,$

где $a -$ биты двоичных данных

$c -$ codeword

$$c_1 = (0\ 1\ 1\ 1\ 0) \oplus \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0&0&0 \\ 1&1&0&1&0&0&1&0&0 \\ 1&0&0&0&0&0&0&1&1 \end{pmatrix} = (0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0)$$

$$c_2 = (0\ 0\ 0\ 1\ 1) \oplus \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0&0&0 \\ 1&1&0&1&0&0&1&0&0 \\ 1&0&0&0&0&0&0&1&1 \end{pmatrix} = (0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1)$$

$$c_3 = (0\ 1\ 1\ 1\ 1) \oplus \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0&0&0 \\ 1&1&0&1&0&0&1&0&0 \\ 1&0&0&0&0&0&0&1&1 \end{pmatrix} = (1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1)$$

$$c_4 = (0\ 1\ 0\ 1\ 1) \oplus \begin{pmatrix} 1&1&1&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0 \\ 0&1&0&1&0&1&0&0&0 \\ 1&1&0&1&0&0&1&0&0 \\ 1&0&0&0&0&0&0&1&1 \end{pmatrix} = (1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1)$$

Двоичный код теперь будет таким: 000111100 010100111 100111111 110010111

d. Сымитируем вредоносное вмешательство в закодированное сообщение.

→ 1 какой-нибудь бит:

000110100 010100111 100111111 110010111

→ 2 каких-нибудь бита;

000111100 011100101 100111111 110010111

→ 3 каких-нибудь бита;

000110100 010100101 100111011 110010111

→ 4 каких-нибудь бита.

000110100 010100101 100111011 110010011

е. Декодируем

Чтобы легко декодировать кодированное сообщение, мы можем использовать матрицу R. Это матрица, умноженная на G равна единичной матрице

$$R = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Мы используем формулу $d = cR$, где d – данный бит

1. в 1 – м случае **000110100 010100111 100111111 110010111**

$$d_1 = (0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (0 \quad 1 \quad 0 \quad 1 \quad 0)$$

→ 01010 / 00011 / 01111 / 01011↔йнок

2. **в 2-м случае 000111100 011100101 100111111 110010111**

$$d_2 = (0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (1 \quad 0 \quad 0 \quad 1 \quad 1)$$

→ 01110 / 10011 / 01111/ 01011 ↔ нток

3. **в 3-м случае 000110100 010100101 100111011 110010111**

$d_1 = (0 \quad 1 \quad 0 \quad 1 \quad 0)$

$$d_2 = (0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (0 \quad 0 \quad 0 \quad 1 \quad 1)$$

$$d_3 = (1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1)\begin{pmatrix}0&0&0&0&0\\0&0&0&0&0\\1&0&0&0&0\\0&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&0\\0&0&0&0&1\end{pmatrix} = (0\ \ 1\ \ 1\ \ 0\ \ 1)$$

→ *01010 | 00011 | 01101| 01011 ↔ йгмк*

4. **в 4-м случае 00011<u>0</u>100 0101001<u>0</u>1 1001110<u>1</u>11 1100100<u>1</u>11**

$d_1 = (0\ \ 1\ \ 0\ \ 1\ \ 0)$

$d_2 = (0\ \ 0\ \ 0\ \ 1\ \ 1)$

$d_3 = (0\ \ 1\ \ 1\ \ 0\ \ 1)$

$$d_4 = (1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1)\begin{pmatrix}0&0&0&0&0\\0&0&0&0&0\\1&0&0&0&0\\0&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&0\\0&0&0&0&1\end{pmatrix} = (0\ \ 1\ \ 0\ \ 0\ \ 1)$$

→ *01010 | 00011 | 01101| 01001 ↔ йгми*

f. Найти и исправить ошибки через матрицу H

- **1 какой-нибудь бит - 00011<u>0</u>100 010100111 100111111 110010111**

$$s_1 = \begin{pmatrix}1&0&1&0&1&0&1&0&1\\0&1&1&0&0&1&1&0&0\\0&0&0&1&1&1&1&0&0\\0&0&0&0&0&0&0&1&1\end{pmatrix} \oplus \begin{pmatrix}0\\0\\0\\1\\1\\0\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\1\\0\end{pmatrix}$$

Формула: $s = H \oplus r$

где $s -$ синдром вектор

$r = c^T$

s соответствует 6-му столбцу матрицы H и в своей конструкции так, что синдром 0110 соответствует двоичному значению 6, что указывает на то, что 6-ый бит поврежден.

$$\rightarrow r_{corrected} = \begin{pmatrix}0\\0\\0\\1\\1\\\overline{0}\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\\1\\1\\1\\0\\0\end{pmatrix}$$

$$s_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{ошибок нет}$$

$$s_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{ошибок нет}$$

$$s_4 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{ошибок нет}$$

- **2 каких-нибудь бита - 000111100 01110010**1 **100111111 110010111**

$$s_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{ошибок нет}$$

$$s_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

$$s_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{ошибок нет}$$

$$s_4 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{ошибок нет}$$

→ При таком декодировании неправильное положение обнаружить невозможно. Следовательно, наш декодер не только не исправит ошибок в позициях, в которых они произошли, но и внесет ошибку в ту позицию, где ее не было. Таким образом $(9, 5)$код не обеспечивает исправления двойных ошибок, а также ошибок большей кратности

- **3 каких-нибудь бита: 000110100 010100101 100111011 110010111**

$$s_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rightarrow r_{1-corrected} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ \overline{0} \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$s_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \rightarrow r_{2-corrected} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ \overline{0} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$s_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rightarrow r_{3-corrected} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ \overline{1} \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$s_4 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \text{ошибок нет}$$

- **4 каких-нибудь бита: 000110100 010100101 100111011 110010011**

$$s_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rightarrow r_{1-corrected} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ \bar{1} \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$s_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \rightarrow r_{2-corrected} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ \bar{0} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$s_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rightarrow r_{3-corrected} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ \bar{1} \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$s_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \rightarrow r_{3-corrected} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ \bar{1} \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Задание 4. Код Хэмминга?

1. **Как решить головоломку с монетами с помощью линейной алгебры**

Вам и вашему сокамернику предоставляется шахматная доска с монетами на каждой клетке. Один из вас знает, где спрятан ключ, а другой должен определить его местонахождение на основе рисунка орла и решки на шахматной доске. Перед выходом из комнаты разрешено подбросить только одну монету. Надзиратель может подслушать вашу стратегию и попытаться помешать вам, расположив монеты и ключ определенным образом.

Загадку с монетами можно решить с помощью линейной алгебры, выразив задачу в виде системы линейных уравнений. Пусть H — матрица, в которой каждая строка представляет возможное состояние монеты, а каждый столбец — отдельный квадрат на доске. Элемент $h_{i,j}$ матрицы H равен 1, если монета в ячейке j является орлом в состоянии i, и 0 в противном случае.

2. **Как при этом будет выглядеть матрица H?**

Матрица H будет квадратной матрицей размером, равным количеству возможных состояний монеты.

3. **Какая у неё будет размерность?**

Матрица H теперь имеет размер n x n. Разложите монеты в коробки в определенном порядке так, чтобы каждая монета представляла битовое значение 0 или 1.

4. **Какую матричную операцию нужно выполнить второму заключённому, чтобы найти ответ?**

Второй заключенный может найти местоположение ключа, восстановить эту информацию по проверочным битам, помочь обнаружить и исправить ошибки с помощью кодов Хэмминга.