Практическая линейная алгебра

Лабораторная работа №1.

ФИО: Румянцев Алексей Александрович

Номер ИСУ: 368731 Группа: R3241

Поток: Прак. Лин. Ал. 1.3

Приятной проверки!

Задание 1. Шифр Хилла

Алфавит: 0 а 1 б 2 в 3 г 4 д 5 е 6 ё 7 ж 8 з 9 и 10 й 11 к 12 л 13 м 14 н 15 о 16 п 17 р 18 с 19 т 20 у 21 ф 22 х 23 ц 24 ч 25 ш 26 щ 27 ъ 28 ы 29 ь 30 э 31 ю 32 я (пробел) 33 . 34 , 35 ?

N = 37 37 : 1 и : 37 => если число /37, то все ок

Ценное сообщение: ценная смска

Заменим буквы на соответствующие числа: 23 5 14 14 0 32 33 18 13 18 11 0

Составим вектора размерности 2x1

$\begin{pmatrix}23\\5\end{pmatrix}, \begin{pmatrix}14\\14\end{pmatrix}, \begin{pmatrix}0\\32\end{pmatrix}, \begin{pmatrix}33\\18\end{pmatrix}, \begin{pmatrix}13\\18\end{pmatrix}, \begin{pmatrix}11\\0\end{pmatrix}$

$A_{2x2} = \begin{bmatrix}11 & -109\\20 & 48\end{bmatrix}$

$\det A = 11 \cdot 48 + 20 \cdot 109 = 2708 \bmod 37 = 7 \neq 0$

Умножим матрицу A на каждый из векторов и найдем остаток от деления на 37

$\begin{pmatrix}11 & -109\\20 & 48\end{pmatrix}\begin{pmatrix}23\\5\end{pmatrix} = \begin{pmatrix}-292\\700\end{pmatrix} \bmod 37 = \begin{pmatrix}4\\34\end{pmatrix} = \begin{pmatrix}ф\\.\end{pmatrix}$

$\begin{pmatrix}11 & -109\\20 & 48\end{pmatrix}\begin{pmatrix}14\\14\end{pmatrix} = \begin{pmatrix}-1372\\952\end{pmatrix} \bmod 37 = \begin{pmatrix}34\\27\end{pmatrix} = \begin{pmatrix}.\\ъ\end{pmatrix}$

$\begin{pmatrix}11 & -109\\20 & 48\end{pmatrix}\begin{pmatrix}0\\32\end{pmatrix} = \begin{pmatrix}-3488\\1536\end{pmatrix} \bmod 37 = \begin{pmatrix}27\\19\end{pmatrix} = \begin{pmatrix}ъ\\Т\end{pmatrix}$

$\begin{pmatrix}11 & -109\\20 & 48\end{pmatrix}\begin{pmatrix}33\\18\end{pmatrix} = \begin{pmatrix}-1599\\1524\end{pmatrix} \bmod 37 = \begin{pmatrix}29\\7\end{pmatrix} = \begin{pmatrix}ь\\Ж\end{pmatrix}$

$\begin{pmatrix}11 & -109\\20 & 48\end{pmatrix}\begin{pmatrix}13\\18\end{pmatrix} = \begin{pmatrix}-1819\\1124\end{pmatrix} \bmod 37 = \begin{pmatrix}31\\14\end{pmatrix} = \begin{pmatrix}ю\\Н\end{pmatrix}$

$\begin{pmatrix}11 & -109\\20 & 48\end{pmatrix}\begin{pmatrix}11\\0\end{pmatrix} = \begin{pmatrix}121\\220\end{pmatrix} \bmod 37 = \begin{pmatrix}10\\35\end{pmatrix} = \begin{pmatrix}й\\,\end{pmatrix}$

$final_{2x2} =$ ф . . ъ ъ Т ь Ж Ю Н й ,

Для расшифровки сообщения найдем A^{-1}

$$\begin{pmatrix} 11 & -109 \\ 20 & 48 \end{pmatrix}^{-1} = (11\cdot 48 + 20\cdot 109)\begin{pmatrix} 48 & 109 \\ -20 & 11 \end{pmatrix} = \begin{pmatrix} \frac{12}{677} & \frac{109}{2708} \\ -\frac{5}{677} & \frac{11}{2708} \end{pmatrix}$$

Мы знаем, что $A^{-1} = \frac{1}{detA} A^{T}_{ij}$, $detA \cdot \frac{1}{detA} = 1 \bmod N$

Мы можем применить эту формулу поэлементно, тогда

$a^1 \cdot \frac{1}{a} = 1 \bmod N \Rightarrow a^1 \cdot \frac{1}{a} = 1 \bmod 37 \Rightarrow a^1 \cdot \frac{1}{a} = 37n+1$

$a = \frac{12}{677} \Rightarrow a^1 \cdot \frac{677}{12} = 37n+1 \Rightarrow a^1 = \frac{12(37n+1)}{677}$

Простой программой на Python получаем $n = -860 \Rightarrow a^1 = -564$

$b = \frac{109}{2708}$, аналогично $b^1 = \frac{109}{2708}(37n+1)$, $n = 1171$, $b^1 = 1744$

$c = -\frac{5}{677}$, $c^1 = -\frac{5}{677}(37n+1)$, $n = -183$, $c^1 = 50$

$d = \frac{11}{2708}$, $d^1 = \frac{11}{2708}(37n+1)$, $n = 171$, $d^1 = 176$

$$A^{-1} = \begin{pmatrix} -564 & 1744 \\ 50 & 176 \end{pmatrix} \bmod 37 = \begin{pmatrix} 28 & 5 \\ 13 & 28 \end{pmatrix}$$

Вычитательство: ъедъъТьЖЮНЙа

4 5 4 27 27 19 29 7 31 14 10 0

Расшифровка аналогично

$\begin{pmatrix} 28 & 5 \\ 13 & 28 \end{pmatrix}\begin{pmatrix} 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 137 \\ 192 \end{pmatrix} \bmod 37 = \begin{pmatrix} 26 \\ 7 \end{pmatrix} = \begin{pmatrix} \text{Ы} \\ \text{Ж} \end{pmatrix}$

$\begin{pmatrix} 28 & 5 \\ 13 & 28 \end{pmatrix}\begin{pmatrix} 4 \\ 27 \end{pmatrix} = \begin{pmatrix} 247 \\ 808 \end{pmatrix} \vdots 37 = \begin{pmatrix} 25 \\ 31 \end{pmatrix} = \begin{pmatrix} \text{Ш} \\ \text{Ю} \end{pmatrix}$

$\begin{pmatrix} 28 & 5 \\ 13 & 28 \end{pmatrix}\begin{pmatrix} 27 \\ 19 \end{pmatrix} = \begin{pmatrix} 851 \\ 883 \end{pmatrix} \vdots 37 = \begin{pmatrix} 0 \\ 32 \end{pmatrix} = \begin{pmatrix} \text{а} \\ \text{Я} \end{pmatrix}$

$\begin{pmatrix} 28 & 5 \\ 13 & 28 \end{pmatrix}\begin{pmatrix} 29 \\ 7 \end{pmatrix} = \begin{pmatrix} 847 \\ 573 \end{pmatrix} \vdots 37 = \begin{pmatrix} 33 \\ 18 \end{pmatrix} = \begin{pmatrix} \text{пробел} \\ \text{С} \end{pmatrix}$

$\begin{pmatrix} 28 & 5 \\ 13 & 28 \end{pmatrix}\begin{pmatrix} 31 \\ 14 \end{pmatrix} = \begin{pmatrix} 938 \\ 795 \end{pmatrix} \vdots 37 = \begin{pmatrix} 13 \\ 18 \end{pmatrix} = \begin{pmatrix} \text{М} \\ \text{С} \end{pmatrix}$

$\begin{pmatrix} 28 & 5 \\ 13 & 28 \end{pmatrix}\begin{pmatrix} 10 \\ 0 \end{pmatrix} = \begin{pmatrix} 280 \\ 130 \end{pmatrix} \vdots 37 = \begin{pmatrix} 21 \\ 19 \end{pmatrix} = \begin{pmatrix} \text{Ф} \\ \text{Т} \end{pmatrix}$

$vfinal_{2x2} =$ ужин юсл СМСФТ

пробел

$$\exists\, B_{3\times3} = \begin{bmatrix} -1 & 7 & -6 \\ 12 & 3 & 3 \\ 2 & 6 & 8 \end{bmatrix} \quad \det B = -1032 \bmod 37 = 4 \neq 0$$

Составим вектора размерности 3x1 23 5 14 | 14 0 32 | 33 18 13 | 18 11 0

$$\begin{pmatrix} 23 \\ 5 \\ 14 \end{pmatrix}, \begin{pmatrix} 14 \\ 0 \\ 32 \end{pmatrix}, \begin{pmatrix} 33 \\ 18 \\ 13 \end{pmatrix}, \begin{pmatrix} 18 \\ 11 \\ 0 \end{pmatrix}$$

Умножим матрицу B на каждый из векторов и найдем остаток от дел. на 37

$$\begin{pmatrix} -1 & 7 & -6 \\ 12 & 3 & 3 \\ 2 & 6 & 8 \end{pmatrix} \begin{pmatrix} 23 \\ 5 \\ 14 \end{pmatrix} = \begin{pmatrix} -72 \\ 333 \\ 188 \end{pmatrix} \bmod 37 = \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} в \\ а \\ г \end{pmatrix}$$

$$\begin{pmatrix} -1 & 7 & -6 \\ 12 & 3 & 3 \\ 2 & 6 & 8 \end{pmatrix} \begin{pmatrix} 33 \\ 18 \\ 13 \end{pmatrix} = \begin{pmatrix} 15 \\ 489 \\ 278 \end{pmatrix} \bmod 37 = \begin{pmatrix} 15 \\ 8 \\ 19 \end{pmatrix} = \begin{pmatrix} о \\ з \\ т \end{pmatrix}$$

$$\begin{pmatrix} -1 & 7 & -6 \\ 12 & 3 & 3 \\ 2 & 6 & 8 \end{pmatrix} \begin{pmatrix} 14 \\ 0 \\ 32 \end{pmatrix} = \begin{pmatrix} -206 \\ 264 \\ 284 \end{pmatrix} \bmod 37 = \begin{pmatrix} 16 \\ 5 \\ 25 \end{pmatrix} = \begin{pmatrix} п \\ е \\ ш \end{pmatrix}$$

$$\begin{pmatrix} -1 & 7 & -6 \\ 12 & 3 & 3 \\ 2 & 6 & 8 \end{pmatrix} \begin{pmatrix} 18 \\ 11 \\ 0 \end{pmatrix} = \begin{pmatrix} 59 \\ 249 \\ 102 \end{pmatrix} \bmod 37 = \begin{pmatrix} 22 \\ 27 \\ 28 \end{pmatrix} = \begin{pmatrix} х \\ ъ \\ ы \end{pmatrix}$$

$final_{3\times3}$ = вагпешозтхъы

аналогично методу с матр. A^{-1} найдем B^{-1}

$$\begin{pmatrix} -1 & 7 & -6 \\ 12 & 3 & 3 \\ 2 & 6 & 8 \end{pmatrix}^{-1} = \begin{pmatrix} -\frac{1}{172} & \frac{23}{258} & \frac{-13}{344} \\ \frac{15}{172} & \frac{-1}{258} & \frac{23}{344} \\ \frac{-11}{172} & \frac{-5}{258} & \frac{29}{344} \end{pmatrix}$$

(elements labelled a, b, c / d, e, f / g, h, k)

$a' = -\frac{1}{172}(37n+1) = /n=79/ = -17$

$b' = \frac{23}{258}(37n+1) = /n = -7/ = -23$

$c' = -\frac{13}{344}(37n+1) = /n = -93/ = 130$

$d' = \frac{15}{172}(37n+1) = /n = 79/ = 255$

$k' = \frac{29}{344}(37n+1) = /n = -93/ = -290$

$e' = -\frac{1}{258}(37n+1) = /n = -7/ = 1$

$f' = \frac{23}{344}(37n+1) = /n = -93/ = -230$

$g' = -\frac{11}{172}(37n+1) = /n = 79/ = -187$

$h' = -\frac{5}{258}(37n+1) = /n = -7/ = 5$

$$B^{-1} = \begin{pmatrix} -17 & -23 & 130 \\ 255 & 1 & -230 \\ -187 & 5 & -290 \end{pmatrix} \bmod 37 = \begin{pmatrix} 20 & 14 & 19 \\ 33 & 1 & 29 \\ 35 & 5 & 6 \end{pmatrix}$$

Вмешательство: в э г п е ш ы з т $_{пробел}$ ъ ы

2 30 3 | 16 5 25 | 28 8 19 | 33 27 28

$$\begin{pmatrix} 20 & 14 & 19 \\ 33 & 1 & 29 \\ 35 & 5 & 6 \end{pmatrix} \begin{pmatrix} 2 \\ 30 \\ 3 \end{pmatrix} = \begin{pmatrix} 517 \\ 183 \\ 238 \end{pmatrix} \% 37 = \begin{pmatrix} 36 \\ 35 \\ 16 \end{pmatrix} = \begin{pmatrix} ? \\ , \\ п \end{pmatrix}$$

$$\begin{pmatrix} 20 & 14 & 19 \\ 33 & 1 & 29 \\ 35 & 5 & 6 \end{pmatrix} \begin{pmatrix} 16 \\ 5 \\ 25 \end{pmatrix} = \begin{pmatrix} 865 \\ 1258 \\ 735 \end{pmatrix} \% 37 = \begin{pmatrix} 14 \\ 0 \\ 32 \end{pmatrix} = \begin{pmatrix} н \\ а \\ я \end{pmatrix}$$

$$\begin{pmatrix} 20 & 14 & 19 \\ 33 & 1 & 29 \\ 35 & 5 & 6 \end{pmatrix} \begin{pmatrix} 28 \\ 8 \\ 19 \end{pmatrix} = \begin{pmatrix} 1033 \\ 1483 \\ 1134 \end{pmatrix} \% 37 = \begin{pmatrix} 34 \\ 3 \\ 24 \end{pmatrix} = \begin{pmatrix} . \\ г \\ ч \end{pmatrix}$$

$$\begin{pmatrix} 20 & 14 & 19 \\ 33 & 1 & 29 \\ 35 & 5 & 6 \end{pmatrix} \begin{pmatrix} 33 \\ 27 \\ 28 \end{pmatrix} = \begin{pmatrix} 1570 \\ 1928 \\ 1458 \end{pmatrix} \% 37 = \begin{pmatrix} 16 \\ 4 \\ 15 \end{pmatrix} = \begin{pmatrix} п \\ д \\ о \end{pmatrix}$$

$v_{final\,3\times3}$ = ?, п н а я . г ч п д о

$$\exists C = \begin{bmatrix} 1 & -7 & -9 & 6 \\ 15 & 23 & 5 & 11 \\ 3 & 2 & -31 & 17 \\ 7 & 10 & 4 & -12 \end{bmatrix}$$

$\det C = 61461 \quad \mod 37 = 4 \neq 0$

Составим вектора размерности 4×1 23 5 14 14 0 32 33 18 13 18 11 0

$$\begin{pmatrix} 23 \\ 5 \\ 14 \\ 14 \end{pmatrix}, \begin{pmatrix} 0 \\ 32 \\ 33 \\ 18 \end{pmatrix}, \begin{pmatrix} 13 \\ 18 \\ 11 \\ 0 \end{pmatrix}$$

Умножим матрицу C на каждый из векторов и найдем остаток от деления на 37

$$\begin{pmatrix} 1 & -7 & -9 & 6 \\ 15 & 23 & 5 & 11 \\ 3 & 2 & -31 & 17 \\ 7 & 10 & 4 & -12 \end{pmatrix} \begin{pmatrix} 23 \\ 5 \\ 14 \\ 14 \end{pmatrix} = \begin{pmatrix} -54 \\ 684 \\ -117 \\ 99 \end{pmatrix} \mod 37 = \begin{pmatrix} 20 \\ 18 \\ 31 \\ 25 \end{pmatrix} = \begin{pmatrix} У \\ С \\ Ю \\ Ы \end{pmatrix}$$

$$\begin{pmatrix} 1 & -7 & -9 & 6 \\ 15 & 23 & 5 & 11 \\ 3 & 2 & -31 & 17 \\ 7 & 10 & 4 & -12 \end{pmatrix} \begin{pmatrix} 0 \\ 32 \\ 33 \\ 18 \end{pmatrix} = \begin{pmatrix} -413 \\ 1099 \\ -653 \\ 236 \end{pmatrix} \mod 37 = \begin{pmatrix} 31 \\ 26 \\ 13 \\ 14 \end{pmatrix} = \begin{pmatrix} Ю \\ Ц \\ М \\ Н \end{pmatrix}$$

$$\begin{pmatrix} 1 & -7 & -9 & 6 \\ 15 & 23 & 5 & 11 \\ 3 & 2 & -31 & 17 \\ 7 & 10 & 4 & -12 \end{pmatrix} \begin{pmatrix} 13 \\ 18 \\ 11 \\ 0 \end{pmatrix} = \begin{pmatrix} -212 \\ 664 \\ -266 \\ 315 \end{pmatrix} \mod 37 = \begin{pmatrix} 10 \\ 35 \\ 30 \\ 19 \end{pmatrix} = \begin{pmatrix} Ц \\ Ь \\ Э \\ Т \end{pmatrix}$$

$final_{4\times4} =$ УСЮШЮЦМНЦЬЭТ

Для расшифровки сообщения найдем C^{-1}

$$\begin{pmatrix} 1 & -7 & -9 & 6 \\ 15 & 23 & 5 & 11 \\ 3 & 2 & -31 & 17 \\ 7 & 10 & 4 & -12 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{3820}{20487} & \frac{1966}{61461} & \frac{-2494}{61461} & \frac{1333}{20487} \\ \frac{-2618}{20487} & \frac{283}{61461} & \frac{2267}{61461} & \frac{-152}{20487} \\ \frac{292}{20487} & \frac{1183}{61461} & \frac{-2251}{61461} & \frac{-563}{20487} \\ \frac{139}{20487} & \frac{1777}{61461} & \frac{-316}{61461} & \frac{-1244}{20487} \end{pmatrix}$$

$a' = \frac{3820}{20487}(37n+1) = /n=5537/ = 38200$

* код на питоне *

```
main.py
a_s = -316
delit = 61461
mod = 37
for n in range(-100000, 100001):
    a = a_s*(mod*n+1)
    if a % delit == 0:
        print(str(n) + " " + str(a/delit))
```

$$C^{-1} = \begin{pmatrix} 38200 & -17694 & 22446 & 13330 \\ -26180 & -2547 & -20403 & -1520 \\ 2770 & -10647 & 20259 & -5630 \\ 1390 & -15993 & 2844 & -12440 \end{pmatrix} \quad mod37 = \begin{pmatrix} 16 & 29 & 24 & 10 \\ 16 & 6 & 21 & 34 \\ 32 & 9 & 20 & 31 \\ 21 & 28 & 32 & 29 \end{pmatrix}$$

Вычитательство: УСПОШЛФУЖНЙ?ЭТ

20 18 31 25 21 26 7 14 10 36 30 19

$$\begin{pmatrix} 16 & 29 & 24 & 10 \\ 16 & 6 & 21 & 34 \\ 32 & 9 & 20 & 31 \\ 21 & 28 & 32 & 29 \end{pmatrix} \begin{pmatrix} 20 \\ 18 \\ 31 \\ 25 \end{pmatrix} = \begin{pmatrix} 1836 \\ 1929 \\ 2197 \\ 2641 \end{pmatrix} \% 37 = \begin{pmatrix} 23 \\ 5 \\ 14 \\ 14 \end{pmatrix} = \begin{pmatrix} Ы \\ Е \\ Н \\ Н \end{pmatrix}$$

$$\begin{pmatrix} 16 & 29 & 24 & 10 \\ 16 & 6 & 21 & 34 \\ 32 & 9 & 20 & 31 \\ 21 & 28 & 32 & 29 \end{pmatrix} \begin{pmatrix} 21 \\ 26 \\ 7 \\ 14 \end{pmatrix} = \begin{pmatrix} 1398 \\ 1115 \\ 1480 \\ 1795 \end{pmatrix} \% 37 = \begin{pmatrix} 29 \\ 5 \\ 0 \\ 23 \end{pmatrix} = \begin{pmatrix} Ь \\ Е \\ А \\ Ы \end{pmatrix}$$

$$\begin{pmatrix} 16 & 29 & 24 & 10 \\ 16 & 6 & 21 & 34 \\ 32 & 9 & 20 & 31 \\ 21 & 28 & 32 & 29 \end{pmatrix} \begin{pmatrix} 10 \\ 36 \\ 30 \\ 19 \end{pmatrix} = \begin{pmatrix} 2114 \\ 1652 \\ 1833 \\ 2729 \end{pmatrix} \% 37 = \begin{pmatrix} 5 \\ 24 \\ 20 \\ 28 \end{pmatrix} = \begin{pmatrix} Е \\ Ч \\ У \\ Ь \end{pmatrix}$$

$Vfinal_{4\times4}$ = ценьеаучь

35%

Задание 2. Взлом Шифра Хилла

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36

алфавит = а б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я пробел . , ? , N = 37

С помощью метода гаусса в главной теме, сгенерируем случайный ключ

$$A=\begin{bmatrix}-7 & 3\\ 12 & 5\end{bmatrix}$$

$\det A = -71 \bmod 37 = 3 \neq 0$

Сообщение 1 = моргенштерн.

Зашифруем сообщение 1

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}13\\ 15\end{pmatrix}=\begin{pmatrix}-46\\ 231\end{pmatrix}\bmod 37=\begin{pmatrix}28\\ 9\end{pmatrix}=\begin{pmatrix}ы\\ и\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}17\\ 3\end{pmatrix}=\begin{pmatrix}-110\\ 219\end{pmatrix}\bmod 37=\begin{pmatrix}1\\ 34\end{pmatrix}=\begin{pmatrix}д\\ .\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}5\\ 14\end{pmatrix}=\begin{pmatrix}7\\ 130\end{pmatrix}\bmod 37=\begin{pmatrix}7\\ 19\end{pmatrix}=\begin{pmatrix}ж\\ т\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}25\\ 19\end{pmatrix}=\begin{pmatrix}-118\\ 395\end{pmatrix}\bmod 37=\begin{pmatrix}30\\ 25\end{pmatrix}=\begin{pmatrix}э\\ ш\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}5\\ 17\end{pmatrix}=\begin{pmatrix}16\\ 145\end{pmatrix}\bmod 37=\begin{pmatrix}16\\ 34\end{pmatrix}=\begin{pmatrix}п\\ .\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}14\\ 34\end{pmatrix}=\begin{pmatrix}4\\ 338\end{pmatrix}\bmod 37=\begin{pmatrix}4\\ 5\end{pmatrix}=\begin{pmatrix}г\\ е\end{pmatrix}$$

$final_{msg1}$ = ыид.жтэшп.ге

Сообщение 2 = Перегудинаа.

Зашифруем сообщение 2

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}16\\ 5\end{pmatrix}=\begin{pmatrix}-97\\ 217\end{pmatrix}\bmod 37=\begin{pmatrix}14\\ 32\end{pmatrix}=\begin{pmatrix}н\\ ь\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}17\\ 5\end{pmatrix}=\begin{pmatrix}-104\\ 229\end{pmatrix}\bmod 37=\begin{pmatrix}7\\ 7\end{pmatrix}=\begin{pmatrix}ж\\ ж\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}3\\ 20\end{pmatrix}=\begin{pmatrix}39\\ 136\end{pmatrix}\bmod 37=\begin{pmatrix}2\\ 25\end{pmatrix}=\begin{pmatrix}в\\ ш\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}4\\ 9\end{pmatrix}=\begin{pmatrix}-1\\ 93\end{pmatrix}\bmod 37=\begin{pmatrix}36\\ 19\end{pmatrix}=\begin{pmatrix}?\\ т\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}14\\ 0\end{pmatrix}=\begin{pmatrix}-98\\ 168\end{pmatrix}\bmod 37=\begin{pmatrix}13\\ 20\end{pmatrix}=\begin{pmatrix}м\\ у\end{pmatrix}$$

$$\begin{pmatrix}-7 & 3\\ 12 & 5\end{pmatrix}\begin{pmatrix}0\\ 34\end{pmatrix}=\begin{pmatrix}102\\ 170\end{pmatrix}\bmod 37=\begin{pmatrix}28\\ 22\end{pmatrix}=\begin{pmatrix}ы\\ х\end{pmatrix}$$

$final_{msg2}$ = НЯЖЖВШ?ТМУЫХ

Забыли сообщение 2 и ключ.

Имеем: $\binom{М}{О}, \binom{Р}{г}, \binom{е}{н}, \binom{ш}{т}, \binom{е}{р}, \binom{Н}{.}$ осн. 1

$\binom{61}{Ц}, \binom{б}{.}, \binom{*}{т}, \binom{э}{ш}, \binom{П}{.}, \binom{g}{e}$ шифр. осн. 1

$\binom{Н}{g}, \binom{*}{*}, \binom{в}{ш}, \binom{?}{т}, \binom{М}{У}, \binom{61}{Х}$ шифр. осн. 2

осн. 2 – ?

Мы знаем, что $\underset{\text{ключ}}{K} \cdot \underset{\text{исходн. вектора}}{P} = \underset{\text{результ. вектора}}{C} \Leftrightarrow K = C \cdot P^{-1}$

Возьмем в качестве P матрицу из любых двух векторов первого основного сообщения.

Единственное условие: $\exists P^{-1}$. Тогда C составится из зашифрованных эквивалентов.

$$\exists P = \begin{pmatrix} М & е \\ О & р \end{pmatrix} = \begin{pmatrix} 13 & 5 \\ 15 & 17 \end{pmatrix}, \quad C = \begin{pmatrix} 61 & П \\ Ц & . \end{pmatrix} = \begin{pmatrix} 28 & 16 \\ 9 & 34 \end{pmatrix} \Rightarrow K = \begin{pmatrix} 28 & 16 \\ 9 & 34 \end{pmatrix} \begin{pmatrix} 13 & 5 \\ 15 & 17 \end{pmatrix}^{-1}, \quad \begin{pmatrix} 13 & 5 \\ 15 & 17 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{17}{146} & \frac{-5}{146} \\ \frac{-15}{146} & \frac{13}{146} \end{pmatrix} \Rightarrow$$

$$\Rightarrow K = \begin{pmatrix} \frac{118}{73} & \frac{34}{73} \\ \frac{-357}{146} & \frac{397}{146} \end{pmatrix}$$

Для расшифровки необходимо найти $K^{-1} \Rightarrow K^{-1} = \begin{pmatrix} \frac{397}{808} & \frac{-17}{202} \\ \frac{357}{808} & \frac{59}{202} \end{pmatrix}$

аналогично методу из задания 1 имеем каждый эл-т

$a' = \frac{397}{808}(37n+1) = 2382 \quad c' = \frac{357}{808}(37n+1) = 2142 \Rightarrow$

$b' = -\frac{17}{202}(37n+1) = 221 \quad d' = \frac{39}{202}(37n+1) = -767$

$$\Rightarrow K^{-1} = \begin{pmatrix} 2382 & 221 \\ 2142 & -767 \end{pmatrix} \vdots 37 = \begin{pmatrix} 14 & 36 \\ 33 & 10 \end{pmatrix}$$

Используя K^{-1} и шифр сообщения 2 найдем исходное сообщение 2

$$\begin{pmatrix}14 & 36\\ 33 & 10\end{pmatrix}\begin{pmatrix}14\\ 32\end{pmatrix}=\begin{pmatrix}1348\\ 782\end{pmatrix} \% 37 = \begin{pmatrix}16\\ 5\end{pmatrix}=\begin{pmatrix}П\\ е\end{pmatrix}$$

$$\begin{pmatrix}14 & 36\\ 33 & 10\end{pmatrix}\begin{pmatrix}7\\ 7\end{pmatrix}=\begin{pmatrix}350\\ 301\end{pmatrix} \% 37 = \begin{pmatrix}17\\ 5\end{pmatrix}=\begin{pmatrix}р\\ е\end{pmatrix}$$

$$\begin{pmatrix}14 & 36\\ 33 & 10\end{pmatrix}\begin{pmatrix}2\\ 25\end{pmatrix}=\begin{pmatrix}928\\ 316\end{pmatrix} \% 37 = \begin{pmatrix}3\\ 20\end{pmatrix}=\begin{pmatrix}2\\ у\end{pmatrix}$$

$$\begin{pmatrix}14 & 36\\ 33 & 10\end{pmatrix}\begin{pmatrix}36\\ 19\end{pmatrix}=\begin{pmatrix}1188\\ 1378\end{pmatrix} \% 37 = \begin{pmatrix}4\\ 9\end{pmatrix}=\begin{pmatrix}д\\ ц\end{pmatrix}$$

$$\begin{pmatrix}14 & 36\\ 33 & 10\end{pmatrix}\begin{pmatrix}13\\ 20\end{pmatrix}=\begin{pmatrix}902\\ 629\end{pmatrix} \% 37 = \begin{pmatrix}14\\ 0\end{pmatrix}=\begin{pmatrix}Н\\ а\end{pmatrix}$$

$$\begin{pmatrix}14 & 36\\ 33 & 10\end{pmatrix}\begin{pmatrix}28\\ 22\end{pmatrix}=\begin{pmatrix}1184\\ 1144\end{pmatrix} \% 37 = \begin{pmatrix}0\\ 34\end{pmatrix}=\begin{pmatrix}а\\ .\end{pmatrix}$$

Итого, получили сообщение перегудинаа., т.т.н.

Задание 3. Код Хэмминга

а - 00000	л - 01100	ъ - 10111
б - 00001	м - 01101	ш - 11000
в - 00010	н - 01110	щ - 11001
г - 00011	о - 01111	ъ - 11010
д - 00100	п - 10000	ы - 11011
е - 00101	р - 10001	ь - 11100
ё - 00110	с - 10010	э - 11101
ж - 00111	т - 10011	ю - 11110
з - 01000	у - 10100	я - 11111
и - 01001	ф - 10101	
й - 01010	х - 10110	
к - 01011		

Закодируем слово "торт"

10011 01111 10001 10011

т о р т

Матрица G зависит от матрицы H

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

перестановки 3-х единиц — Обозначим эту часть как H_{left}

E — проверочные векторы

E $\quad H^T_{left}$

Возьмем $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ переставим столбцы для вида $p_1 p_2 d_1 p_3 d_2 d_3 d_4$

Возьмем $G^T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ Связь с H аналогично примеру

Матрица G составляется по матрице H.
В матрице H находится единичная матрица (векторы в любом порядке) и всевозможные перестановки 3х единиц по строкам. Столбцы единичной матрицы отвечают за биты четности, а столбцы перестановки единиц за биты информации.
Матрица G составляется из единичной матрицы и транспонированной матрицы перестановки единиц из матрицы H (см предыдущ. слайд). При умножении матрицы H на G^T получится нулевая матрица. При перестановке любых столбцев в матрице H необходимо переставить соответствующие строчки в матрице G^T или столбцы в матрице G. Таким образом можно составлять разные H и G^T. Образ матрицы G является ядром матрицы H.

Возьмем по 4 бита и закодируем каждый набор с помощью матрицы G, $C = G^T \cdot V_{\text{столбец}}$

1001 0111 1000 1001

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

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

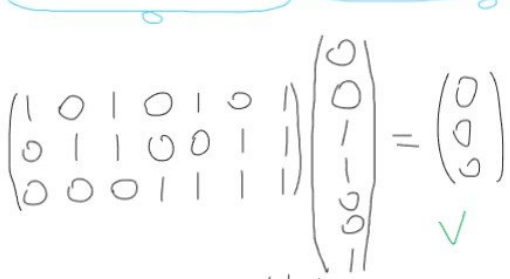
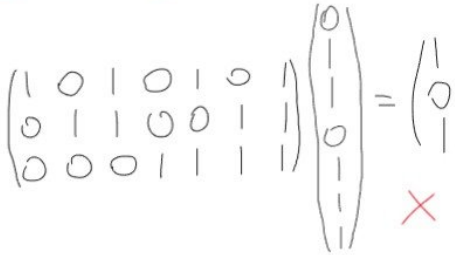
3) $\begin{pmatrix} 1&1&0&1 \\ 1&0&1&1 \\ 1&0&0&0 \\ 0&1&1&1 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

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

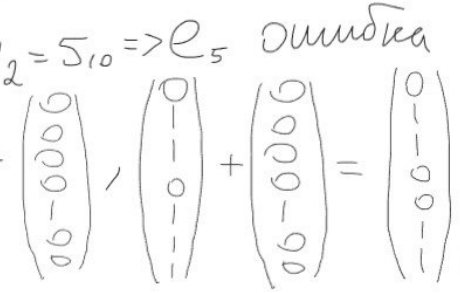
Итого: 0011 0010 1100 1001 0111 0000 1111

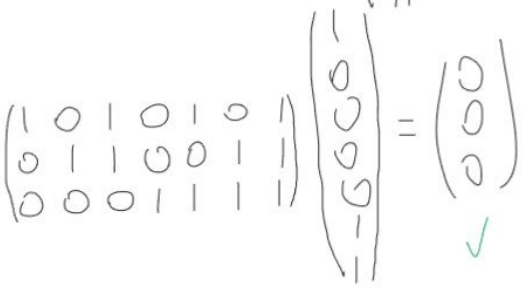
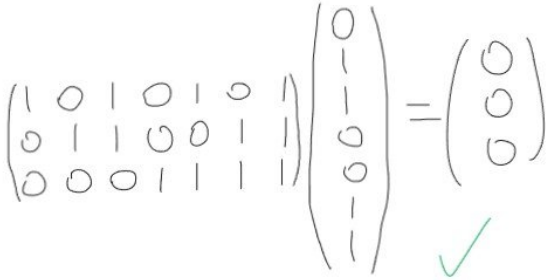
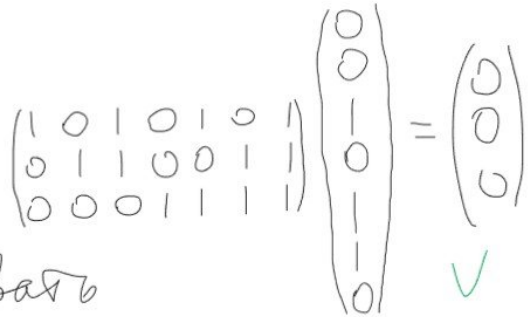
Заменим 1 бит на противоположный в закодированном слове

0011001 0110111 0010110 1000011 1000011

$101_2 = 5_{10} \Rightarrow e_5$ ошибка

$e_5 =$ 

Итого: ошибка исправлена, можно декодировать

~~0~~0~~1~~1001 ~~0~~1~~1~~0011 ~~0~~0~~1~~0110 1000011 1000011

1001 1011 1110 0011 0011

10011 011 1100 1 0011

T O P T

Нет смысла записать биты в одном блоке — поиск ошибок верно работает только с 1ой неверной битом в пределах одного блока.

Также нет смысла проверять не изменение блоки — в них с прошлого раза ничего не изменится.

Заменим 2 бита на противоположные в закодированном слове

00110000 01101110 00100110 10000111

уже правили

$$\begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 0&0&0&1&1&1&1 \end{pmatrix} \begin{pmatrix} 0\\0\\1\\1\\0\\0\\0 \end{pmatrix} = \begin{pmatrix} 1\\1\\1 \end{pmatrix}, \quad 111_2 = 7_{10} \Rightarrow e_7 \text{ ошибка} \Rightarrow e_7 = \begin{pmatrix} 0\\0\\0\\0\\0\\0\\1 \end{pmatrix}, \quad \begin{pmatrix} 0\\0\\1\\1\\0\\0\\0 \end{pmatrix} + \begin{pmatrix} 0\\0\\0\\0\\0\\0\\1 \end{pmatrix} = \begin{pmatrix} 0\\0\\1\\1\\0\\0\\1 \end{pmatrix}$$

X

Итого: ~~00~~1~~1~~001 => 1001

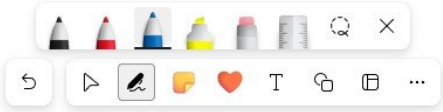
10011 01111 10001 10011

✓

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

✓

T O P T



Заменим 3 бита на противоположные в закодированном слове

00|1000 0110|111 0000|110 0000|011 1000|011

уже правили уже правили

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

Нашли такой же столбец на 3ей позиции => ошибка в 3 бите

Заменяем третий бит на противоположный =>

=> 00|0110

Проверим

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

Итого ~~00~~1~~0~~110 => 1110 ✓

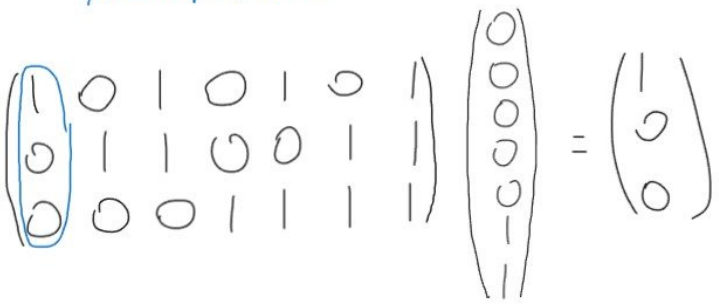
1001|1011|1000|1011

Т О Р Т

Заменим 4 бита на противоположные в закодированном слове

00110000 01101111 00001100 00000011 10000011

уже правим уже правим уже правим

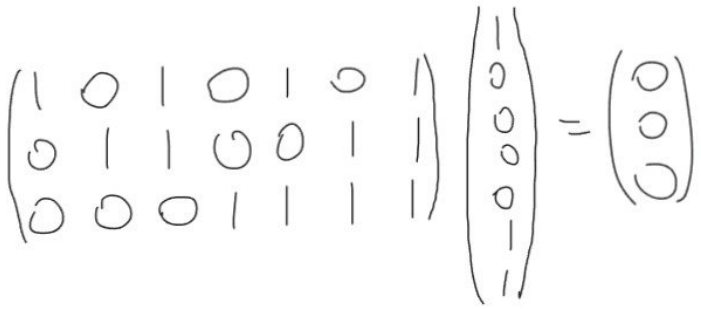


/аналогично предыдущему пункту/

=> заменим первый бит на противоположный =>

=> 10000011

Проверим



Итого: ~~10~~0000~~11~~ => 0011

10011 01111 10001 10011

Т О Р Т