Оглавление

[Криптосистема Хилла 2](#_Toc53982573)

[Пример-шифрование 2](#_Toc53982574)

[Пример-расшифрование 3](#_Toc53982575)

[Задание 1 4](#_Toc53982576)

[Задание 2 5](#_Toc53982577)

[Задание 3 5](#_Toc53982578)

[Задание 4 5](#_Toc53982579)

[Задание 5 5](#_Toc53982580)

[Задание 6 5](#_Toc53982581)

[Задание 7 5](#_Toc53982582)

[Задание 8 5](#_Toc53982583)

# Криптосистема Хилла

Шифр замены. Только замена выполняется не символа на символ, а блока символов на блок символов. Такой шифр называют блочным. Рассмотрим случай, когда блок состоит из двух символов. Идея замены была предложена Хиллом в статьях: L. S. Hill, "Concerning certain linear transformation apparatus of cryptography", American Mathematical Monthly, Volume 38 (1931), 135-154. Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly Vol.36, June–July 1929, pp. 306–312.

### Пример-шифрование

Рассмотрим сообщение:

THE GOLD IS BURIED IN ORONO.

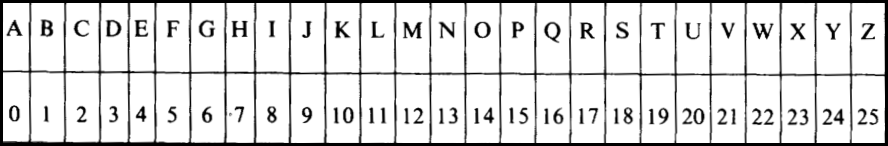
Сформируем блоки по 2 символа:

TH EG OL DI SB UR IE DI NO RO NO.

Т.к. у каждого символа есть свой числовой эквивалент (табл.1), то полученные блоки будут выглядеть так:

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8 13 14 17 14 13 14.

Таблица 1



Каждый блок из двух чисел  исходного сообщения преобразуется в блок из двух чисел  зашифрованного сообщения по следующей формуле:



где , , А – матрица размерности 2x2.

Пусть , тогда шифрование первого блока  будет выглядеть так:



где 



Если применить эту формулу ко всем блокам, то получим следующий результат:

6 25 18 2 23 13 21 2 3 9 25 23 4 14 21 2 17 2 1l l8 l7 2.

Или в символьном виде:

GZ SC XN VC DJ ZX EO VC RC LS RC.

### Пример-расшифрование

Расшифрование выполняется по формуле:

,

где  - обратная к матрица по mod 26.

Для матрицы



если определитель



является взаимно простым со значением модуля (в данном случае 26), то

обратную матрицу  можно найти по следующей формуле:



где  - обратное значение по умножению для  по модулю 26.

Для матрицы  обратная по модулю 26 будет матрица

.

Тогда, расшифровка, например, первого зашифрованного блока будет такой:

,

где 



## Задание 1

Расшифровать файл im3\_hill\_c\_all.bmp. Ключ – матрица K=[[189 58]

[ 21 151]].

## Задание 2

Расшифровать файл m18\_hill\_c\_all.bmp. Шифр Хилла. Режим ECB. K=[[ 47 239] [119 108]]. Зашифровать, оставив первые 50 байт без изменения.

## Задание 3

Расшифровать файл m19\_hill\_cbc\_c\_all.bmp. Шифр Хилла. Режим CBC. K=[[139 194] [185 251]], iv=(34, 56). Зашифровать, оставив первые 50 байт без изменения.

## Задание 4

Расшифровать файл m20\_hill\_ofb\_c\_all.bmp. Шифр Хилла. Режим OFB. K=[[206 9] [207 155]], iv=(144, 215). Зашифровать, оставив первые 50 байт без изменения.

## Задание 5

Расшифровать файл m21\_hill\_cfb\_c\_all.bmp. Шифр Хилла. Режим CFB. K=[[134 69] [ 35 23]], iv=(32, 187). Зашифровать, оставив первые 50 байт без изменения.

## Задание 6

Дешифровать файл p1\_hill\_c\_all.png. Шифр Хилла. Режим ECB.

## Задание 7

Дешифровать png-файл b4\_hill\_c\_all.png. Первые четыре байта в любом png-файле: 137, 80, 78, 71.

## Задание 8

Дешифровать файл text2\_hill\_c\_all.txt. Известно, что текст в файле начинается со слова Whose.