Оглавление

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

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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

Каждый блок из двух чисел $\begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$ исходного сообщения преобразуется в блок из двух чисел $\begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$ зашифрованного сообщения по следующей формуле:

$$C \equiv AP \pmod{26}$$

где $C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix}$, $P = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix}$, A – матрица размерности 2x2.

Пусть $A = \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$, тогда шифрование первого блока $P = \begin{bmatrix} 19 \\ 7 \end{bmatrix}$ будет выглядеть так:

$$C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \equiv \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix} \begin{bmatrix} 19 \\ 7 \end{bmatrix} \pmod{26}$$

где $C_1 \equiv 5 \cdot 19 + 17 \cdot 7 \equiv 6 \pmod{26}$

$C_2 \equiv 4 \cdot 19 + 15 \cdot 7 \equiv 25 \pmod{26}$

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 11 18 17 2.

Или в символьном виде:

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

Пример-расшифрование

Расшифрование выполняется по формуле:

$$P \equiv A^{-1}C \pmod{26},$$

где A^{-1} - обратная к A матрица по mod 26.

Для матрицы

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

если определитель

$$\Delta = \det \mathrm{A} = ad - bc$$

является взаимно простым со значением модуля (в данном случае 26), то обратную матрицу A^{-1} можно найти по следующей формуле:

$$\mathrm{A}^{-1} = \Delta^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

где Δ^{-1} - обратное значение по умножению для Δ по модулю 26.

Для матрицы $\mathrm{A} = \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$ обратная по модулю 26 будет матрица

$$\mathrm{A}^{-1} = \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix}.$$

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

$$\mathrm{P} = \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \equiv \begin{pmatrix} 17 & 5 \\ 18 & 23 \end{pmatrix} \begin{bmatrix} 6 \\ 25 \end{bmatrix} (\mathrm{mod}\, 26),$$

где $P_1 \equiv 17 \cdot 6 + 5 \cdot 25 \equiv 19 \ (\mathrm{mod}\, 26)$

$P_2 \equiv 18 \cdot 6 + 23 \cdot 25 \equiv 7 \ (\mathrm{mod}\, 26)$

Задание1

Расшифроватьфайлim3_hill_c_all.bmp. Ключ – матрицаK=[[189 58] [21 151]].

Задание 2

Расшифроватьфайлm18_hill_c_all.bmp. ШифрХилла.K=[[47 239] [119 108]]. Зашифровать, оставив первые 50 байт без изменения.

Задание 3

Дешифроватьфайлp1_hill_c_all.png. ШифрХилла.

Задание 4

Дешифровать png-файл b4_hill_c_all.png. Первые четыре байта в любом png-файле: 137, 80, 78, 71.

Задание 5

Дешифроватьфайлtext2_hill_c_all.txt. Известно, что текст в файле начинается со слова Whose.