Шифр Хилла

Кевролетин В.В.

12 декабря 2011 г.

Задание 3.2.1

Условие

Каковы необходимые и достаточные условия взаимной однозначности преобразования Хилла?

Решение

Существование обратной матрицы для матрицы при помощи котороый осуществляется шифрование.

Задание 3.2.2

Условие

Если det A= -1 mod 26, то A – 2*2 матрица инволюций т. и т. т., когда $a_{11} + a_{22} = 0 mod 26$. Построить матрицу инволюций при $a_{11} = 2$

Решение

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 13 \end{pmatrix}$$

Проверяем:

$$det(A)(mod\ 26) = 2 * 13 - 1(mod\ 26) = -1(mod\ 26)$$

Задание 3.2.3

Условие

Какова методика криптоанализа шифра Хилла с избранным открытым текстом?

Решение

При известном открытом тексте, размерности матрицы и криптотексте строится система линейных уравнений, решение которой даёт обратную матрицу. Продемонстрируем на примере:

Открытый тест: HELP

Криптотекст: HIAT

Тогда, обозначив за M исходную матрицу, используемую при шифровании, и как и при шифровании записав вместо букс их порядковые номера получим:

$$M \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix}$$

$$M \begin{pmatrix} 11 \\ 15 \end{pmatrix} = \begin{pmatrix} 0 \\ 9 \end{pmatrix}$$

Решив данную системы найдём M:

$$\begin{pmatrix} 2 & 3 \\ 2 & 5 \end{pmatrix}$$