НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н. Тихонова

# КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

**Задания (с разбором): материал 17**

## Матричный шифр Хилла

**Евсютин О.О.**

Москва 2020

## 1 ЦЕЛЬ РАБОТЫ

Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к блочному шифру Хилла.

## 2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Шифр Хилла представляет собой пример блочного шифра, основанного на матричных преобразованиях с использованием арифметики остатков. Данный шифр устроен следующим образом.

Открытый текст разбивается на блоки длиной $n$, и каждый блок представляется в виде $n$-мерного вектора.

Ключом является квадратная матрица размера $n \times n$.

$\mathbb{K} = GL_n(\mathbb{Z}_m)$.

$K = \left(k_{i,j}\right),\ i,j = \overline{1,n},\ k_{i,j} \in \mathbb{Z}_m$.

Эта матрица должна быть обратима в $\mathbb{Z}_m$, чтобы была возможна операция расшифрования. Матрица будет являться обратимой только в том случае, если ее детерминант входит в группу обратимых элементов кольца $\mathbb{Z}_m$.

$|K| \in \mathbb{Z}_m^*$.

Операция зашифрования заключается в том, что вектор, соответствующий блоку открытого текста, умножается на ключевую матрицу.

$X = (x_1, \ldots, x_n)^T$.

$$Y = (y_1, \ldots, y_n)^T = E_K(X) = K\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Для того, чтобы расшифровать шифртекст, необходимо, разбив его на блоки, представить каждый блок в виде вектора и умножить на обратную матрицу ключа.

В случае рекуррентного шифра Хилла для каждого блока открытого текста вычисляется новое ключевое значение на основе двух предыдущих.

$K_{i+1} = K_i K_{i-1}$.

$K_{i+1}^{-1} = K_{i-1}^{-1} K_i^{-1}$.

## 3 ЗАДАНИЕ

1) написать программную реализацию следующих шифров:
   - шифр Хилла;
   - рекуррентный шифр Хилла;
2) изучить методы криптоанализа матричных шифров с использованием дополнительных источников;
3) провести криптоанализ данных шифров;
4) подготовить отчет о выполнении работы.

Программа должна обладать следующей функциональностью для каждого из реализованных в ней шифров:

1) принимать на вход произвольную последовательность символов, вводимую пользователем в качестве открытого текста или шифртекста;
2) принимать на вход секретный ключ вида, соответствующего конкретному шифру;

3) осуществлять зашифрование или расшифрование введенного текста по выбору пользователя.

Отчет должен содержать следующие составные части:

1) раздел с заданием;
2) раздел с краткой теоретической частью;
3) раздел с двумя-тремя примерами «ручного» шифрования для произвольных последовательностей символов;
4) раздел с результатами работы программы для тех же последовательностей символов, что и в предыдущем разделе;
5) раздел с примерами криптоанализа реализованных шифров;
6) раздел с выводами о проделанной работе.