НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

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

**КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**Практическая работа 2**

**Подстановочные шифры**

**Евсютин О.О.**

Москва 2025

**1 ЦЕЛЬ РАБОТЫ**

Целью данной работы является приобретение навыков программной реализации и криптоанализа применительно к простым подстановочным шифрам.

**2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

Простейшим примером подстановочного шифра является шифр простой замены.

Математически данный шифр может быть описан на языке подстановок.

Каждой букве алфавита мощностью ставится в соответствие число из диапазона — другими словами, все символы алфавита нумеруются.

Множество возможных ключей шифра простой замены является симметрической группой степени , то есть группой подстановок длины : .

Открытый текст обозначим , где , , соответствующий шифртекст — .

Зашифрование открытого текста на ключе может быть записано как , расшифрование шифртекста на том же ключе — , где — подстановка, обратная .

Проще говоря, при зашифровании каждый символ текста заменяется на другой символ с помощью ключевой подстановки.

Известным частным случаем шифра простой замены является шифр Цезаря, названный так по имени использовавшего его всю жизнь древнеримского полководца. Данный шифр основан на использовании одного-единственного ключа — подстановки, полученной циклическим сдвигом элементов второй строки относительно первой на три позиции влево.

Другим частным случаем шифра простой замены является аффинный шифр, основанный на так называемом аффинном преобразовании.

Данный шифр реализует замену символов открытого текста с использованием операций в кольце классов вычетов. Символы алфавита мощностью представляются элементами кольца классов вычетов .

В качестве ключа аффинного шифра выступает пара значений , , , соответственно ключевое пространство имеет вид .

Открытый текст и шифртекст обозначим соответственно и  
, где , , .

Зашифрование отдельного символа открытого текста осуществляется по формуле , , расшифрование — по формуле , .

Усилением аффинного шифра является аффинный рекуррентный шифр, когда для каждого символа открытого текста вычисляется новое ключевое значение на основе предыдущего. Для этого необходимо задать две ключевые пары ,  
, и тогда ключевая пара для произвольного символа преобразуемой последовательности будет иметь вид , .

Аффинный шифр может быть реализован не только в кольце классов вычетов , но и в иных алгебраических структурах, в частности, в поле Галуа . Возможны два способа представления символов сообщения в виде элементов поля Галуа:

* Параметры поля Галуа выбираются таким образом, чтобы значение соответствовало мощности используемого алфавита. Это не всегда возможно для алфавитов естественных языков, поэтому можно работать с усеченным или расширенным алфавитом.
* Независимо от используемого алфавита естественного языка сообщение представляется в виде двоичной последовательности, которая разбивается на -разрядные блоки. Отдельно взятый блок рассматривается как символ сообщения, подлежащий замене с помощью подстановочного шифра. Алфавит, составленный из таких символов, будет иметь мощность , поэтому он может быть представлен в виде поля Галуа .

В качестве ключа аффинного шифра, построенного над полем Галуа , выступает пара значений , , , и ключевое пространство имеет вид  
. Формулы, определяющие зашифрование и расшифрование, ничем не отличаются от соответствующих формул, введенных ранее для аффинного шифра в кольце классов вычетов .

**3 ЗАДАНИЕ**

1. написать программную реализацию следующих шифров:

- шифр простой замены:

- аффинный шифр;

- аффинный рекуррентный шифр;

1. изучить методы криптоанализа моноалфавитных подстановочных шифров с использованием дополнительных источников;
2. провести криптоанализ данных шифров;
3. подготовить отчет о выполнении работы.

Аффинный шифр и аффинный рекуррентный шифр должны быть реализованы в кольце классов вычетов .

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 примером «ручного» (без использования программных средств) шифрования и расшифрования для произвольных последовательностей символов;
4. раздел с программным кодом и результатами работы программы для тех же последовательностей символов, что и в предыдущем разделе. Допускается представление программного кода отдельно от отчёта в виде дополнительного файла либо размещение в отчёте ссылки на программный код;
5. раздел с примерами криптоанализа реализованных шифров;
6. раздел с выводами о проделанной работе.