НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

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

**КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

**Практическая работа 3**

**Построение криптографических операций в полях Галуа**

**Евсютин О.О.**

Москва 2025

**1 ЦЕЛЬ РАБОТЫ**

Целью данной работы является приобретение навыков программной реализации операций над многочленами в полях Галуа для построения криптографических преобразований.

**2 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

**2.1 Поля Галуа**

Полем Галуа называется поле , полученное расширением простого конечного поля посредством неприводимого многочлена степени . Мощность поля Галуа составляет . Элементами поля Галуа являются многочлены, принадлежащие кольцу многочленов над полем , степень которых строго меньше . Принадлежность многочлена кольцу многочленов означает, что коэффициенты при степенях данного многочлена являются элементами поля . Таким образом, поле Галуа состоит из всевозможных остатков от деления многочленов, заданных над полем , на неприводимый многочлен степени , и в общем случае может быть записано так:  
.

В поле Галуа определены две операции: сложение и умножение.

Чтобы сложить два многочлена–элемента поля Галуа , необходимо сложить их коэффициенты при соответствующих степенях и привести полученные значения по модулю .

Чтобы перемножить два многочлена–элемента поля Галуа , необходимо каждый член одного многочлена умножить на каждый член второго многочлена, привести подобные, привести коэффициенты при степенях полученного многочлена по модулю и выполнить деление полученного многочлена, степень которого может быть выше , на неприводимый многочлен степени . Остаток от такого деления и будет представлять собой результат перемножения двух исходных элементов поля Галуа.

Известно, что мультипликативная группа поля Галуа , включающая все ненулевые элементы поля, представляет собой циклическую группу порядка . Это означает, что каждый элемент данной группы может быть представлен в виде некоторой степени образующего элемента : . Количество образующих элементов группы может быть определено через функцию Эйлера как . Разложение элементов мультипликативной группы поля Галуа по степеням образующего позволяет реализовать операцию умножения многочленов в поле Галуа более простым образом. Пусть даны два многочлена , причем известно, что , . Тогда умножение данных многочленов может быть выполнено по следующей формуле:

|  |  |
| --- | --- |
| . | (1) |

**2.2 Построение аффинного шифра над полем Галуа**

Математический аппарат полей Галуа широко используется для конструирования криптографических операций в современных симметричных шифрах. В качестве основных примеров можно привести шифры AES и Кузнечик. В шифре AES один из этапов основного криптографического преобразования состоит в замене байтов мультипликативно обратными значениями в группе . В шифре Кузнечик в качестве одного из базовых преобразований используется свертка 16-байтового слова в один байт посредством линейного преобразования в поле Галуа .

Наиболее простым примером шифра, который может быть построен над полем Галуа, является аффинный шифр, основанный на так называемом аффинном преобразовании.

Пусть – это алфавит, используемый для представления сообщений, подлежащих шифрованию. Символы данного алфавита представляются в виде элементов поля Галуа одним из двух возможных способов:

* Параметры поля Галуа выбираются таким образом, чтобы выполнялось равенство . 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 аффинного шифра. Алфавит, составленный из таких символов, будет иметь мощность , поэтому он может быть представлен в виде поля Галуа .

Тогда открытый текст после перехода от исходного алфавита к полю Галуа может быть обозначен , соответствующий шифртекст – , где , . В качестве ключа аффинного шифра, построенного над полем Галуа , выступает пара значений , , , и ключевое пространство имеет вид .

Зашифрование отдельного символа открытого текста осуществляется по следующей формуле:

|  |  |
| --- | --- |
| , . | (2) |

Расшифрование символа шифртекста осуществляется по формуле

|  |  |
| --- | --- |
| , , | (3) |

где – элемент поля Галуа, мультипликативно обратный к .

**3 ЗАДАНИЕ**

1. написать программную реализацию инструмента, позволяющего строить и исследовать поле Галуа (без использования готовых библиотечных решений);
2. написать программную реализацию аффинного шифра над полем Галуа ;
3. подготовить отчет о выполнении работы.

Инструмент для построения и исследования полей Галуа должен обладать следующей функциональностью:

1. принимать на вход значения и , определяющие поле Галуа, и строить и отображать соответствующее поле Галуа ;
2. принимать на вход неприводимый многочлен степени либо генерировать такие многочлены для заданных значений и ;
3. принимать на вход многочлены–элементы поля Галуа и осуществлять их сложение или умножение по выбору пользователя;
4. находить образующие элементы мультипликативной группы поля Галуа и выполнять разложение элементов данной группы по степеням выбранного образующего.

Программная реализация аффинного шифра должна обладать следующей функциональностью:

1. принимать на вход произвольную последовательность символов, вводимую пользователем в качестве открытого текста или шифртекста;
2. принимать на вход секретный ключ , , ;
3. осуществлять зашифрование или расшифрование введенного текста по выбору пользователя.

Отчет должен содержать следующие составные части:

1. раздел с заданием;
2. раздел с краткими теоретическими сведениями;
3. раздел с программным кодом и описанием особенностей программных реализаций. Допускается представление программного кода отдельно от отчёта в виде дополнительного файла либо размещение в отчёте ссылки на программный код;
4. раздел с демонстрацией примеров работы программных реализацией и объяснением полученных результатов;
5. раздел с выводами о проделанной работе.