Практическая работа №2

Изучение математических основ криптографии[1]

Цели и задачи работы: изучение циклических алгоритмов, операторов цикла, программирование циклического вычислительного процесса на примере математических методов основ криптографии.

Задание к работе: Реализовать циклический вычислительный процесс. Самостоятельно решить задачи в соответствии с индивидуальным вариантом.

Методика выполнения работы:

1. Разработать алгоритм решения задачи по индивидуальному заданию.
2. Написать и отладить программу решения задачи.
3. Протестировать работу программы на различных исходных данных.
4. Ответить на вопросы по выполненным заданиям, по запросу преподавателя модифицировать код.
5. Ответить на вопросы согласно списку понятий к защите практики (с численными примерами).
6. По запросу преподавателя решить практическое задание на тему «Изучение математических основ криптографии».

Задание 1. Реализовать $a^x \bmod p$ Сравнения по модулю простого числа через теорему Ферма и свойства сравнений. Программа должна проверять условия выполнения теоремы Ферма и простоту вводимого пользователем модуля. Реализовать алгоритм через разложение степени в двоичный вид (логарифм)[2].

Задание 2. Реализовать алгоритм Евклида для вычисления $c*d \bmod m=1$ (через u и v).

Задание 3. Реализовать алгоритм Евклида для вычисления взаимообратного числа $c^{-1} \bmod m=d$.

Задание 4. Написать программу, использующую алгоритм шифрования данных для преобразования исходного текста[3].

Вариант 1 - Диффи-Хеллмана
Вариант 2 - Шамира
Вариант 3 - Эль-Гамаля
Вариант 4 – RSA
Вариант 5 - Хьюза (Hughes)

Задание 5. Написать алгоритм представления числа в виде

[1] На двух ЯП
[2] Два алгоритма
[3] Выбор варианта по модулю 5 по списку группы

цепной дроби. Решить в целых числах уравнения:

Ъ × а + Ь × б = D:

Вариант 1 – 143а+169б=5
Вариант 2 – 275а+145б=10
Вариант 3 – 1256а+847б=119
Вариант 4 – 237а+44б=1
Вариант 5 – 439а+118б=3

Задание 6. Продемонстрировать эмуляцию атаки на базе программы задания 4 данной практической работы.

Задание 7. Написать сообщение на тему «Стандарты современной криптографии в РФ».

Список понятий к защите практики. Множество. Алгебра. Носитель алгебры. Тип алгебры. Сигнатура алгебры. Группа. Кольцо. Ассоциативное кольцо. Кольцо с единицей. Коммутативное кольцо. Поле. Делимость в кольце целых чисел (факт делимости, математическая запись). Отношение сравнения (свойства, теорема (4 пункта)). Рефлексивность, симметричность и транзитивность отношения сравнения. Критерий сравнимости. Простые числа, теорема о свойствах простых чисел. Распределение простых чисел (Эратосфен). Основная теорема арифметики. Функция Эйлера, определение и основные свойства. Каноническое разложение числа. Функция Эйлера (вычисление по определению и через каноническое разложение числа). Теорема об остатках двух чисел и операции Ъ. Теорема Эйлера. Теорема Ферма. Алгоритм Евклида (математическая запись). Наибольший общий делитель – алгоритм Евклида (через u и v, с примером). Расширенный алгоритм Евклида. Обобщенный алгоритм Евклида. Алгоритм возведения числа в степень по модулю (простого числа) с математическим обоснованием (два алгоритма, с примерами). Нахождение числа, обратного по модулю ($a^{-1} \bmod p$).

Криптография. Стеганография. Классическая задача передачи сообщений от некоторого отправителя А к получателю В. Классическая система секретной связи. Односторонняя функция. Дискретный логарифм. Первая система с открытым ключом – криптопротокол Диффи-Хеллмана. Криптопротокол Шамира. Криптопротокол Эль-Гамаля. Криптопротокол RSA.

Удостоверяющий центр. Симметричная криптография (плюсы, минусы, особенности). Ассиметричная криптография

(плюсы, минусы, особенности). Стандарты криптографии. Схема шифрования с открытым ключом (плюсы, минусы).