МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ _____

ПРЕПОДАВАТЕЛЬ

ассистент	_____	Исаева М.Н.
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №6

Криптографические протоколы

по курсу: Криптографические методы защиты информации

СТУДЕНТ ГР. № 5912	_____	Нам Д. О.
номер группы	подпись, дата	инициалы, фамилия

Санкт-Петербург
2022

1. Цель работы

Реализовать схему разделения секрета на китайской теореме об остатках. Разработка двух независимых модулей: первый должен принимать на вход секрет и возвращать его проекции, второй должен брать проекции и возвращать секрет. Отчет должен содержать описание протокола с указанием особенностей реализации, примеры работы программы.

2. Описание алгоритма:

Для реализации схемы разделения секрета на китайской теореме об остатках будет использована схема Миньотта. Совместное использование секрета состоит в восстановлении секрета S из набора общих ресурсов, каждый из которых содержит частичную информацию о секрете. Китайская теорема об остатках (CRT) утверждает, что для данной системы уравнений решение уникально. Таким образом, совместное использование секретов может использовать китайскую теорему об остатках для получения общих ресурсов, представленных в уравнениях, и секрет может быть восстановлен путем решения системы сравнений, чтобы получить уникальное решение, которое будет секретом для восстановления.

Генерируем последовательность попарно взаимно простых чисел $p_0 < \cdots < p_n$ таких что $p_{n-k+2} \cdot \ldots \cdot p_k < p_1 \cdot \ldots \cdot p_k$.

Затем генерируется случайное целое S такое что $p_{n-k+2} \cdot \ldots \cdot p_k < S < p_1 \cdot \ldots \cdot p_k$. Доли вычисляются как $I_i = S \bmod p_i$, где i от 1 до n. Полученные доли используются для китайской теоремы об остатках.

$$\begin{cases} x \equiv I_{i_1} \bmod p_{i_1} \\ \vdots \\ x \equiv I_{i_k} \bmod p_{i_k} \end{cases}$$

Решив эту систему, получаем секрет.

3. Описание реализации:

Для работы с большими числами используется библиотека Arbitrary Precision. В данном примере SIZE = 1024, но он может быть увеличен при необходимости.

- generateParams(vector<ap_uint<SIZE>> &p_numbers, int n) – генерация простых чисел, удовлетворяющих условиям $p_0 < \cdots < p_n$ таких что $p_{n-k+2} \cdot \ldots \cdot p_k < p_1 \cdot \ldots \cdot p_k$.
- generateParts(vector<vector<ap_uint<SIZE>>> &pr, vector<ap_uint<SIZE>> &p_numbers, ap_uint<SIZE> S) – вычисление долей
- CRT(vector<vector<ap_uint<SIZE>>> &pr) – китайская теорема об остатках

3. Пример работы программы:

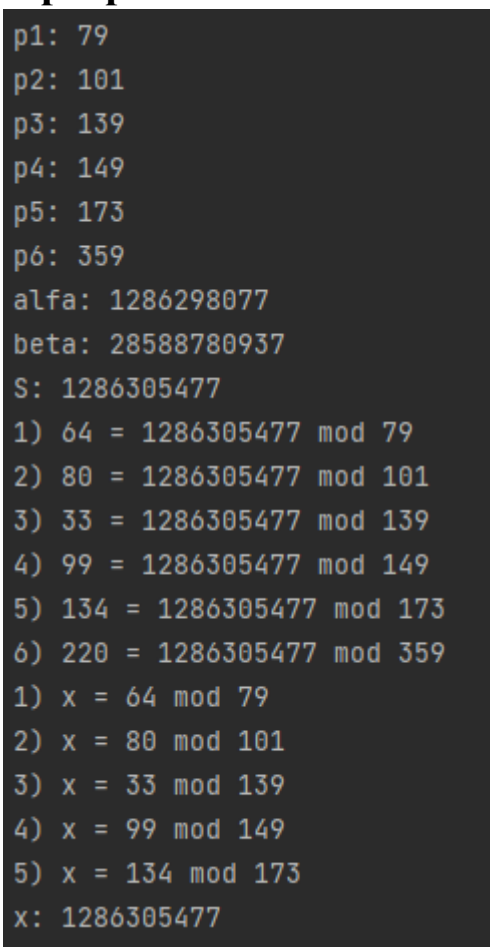

Рис 1. Пример работы программы при n = 6 и k = 5

4. Вывод:

Была реализована схема Миньотта, разделяющая секрет с помощью китайской теоремы об остатках. Поскольку китайская теорема об остатках предоставляет нам метод однозначного определения чисел по модулю относительно простых целых чисел, идея состоит в том, чтобы построить схему, которая определит секрет S с учетом любых k долей (в данном случае остаток от S по модулю каждого из чисел p_i), но не раскроет секрет S, которому дано менее k долей.