Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование асимметричных шифров

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Матюх А.А.

Минск 2020

1. **Теоретические сведения**

В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования (открытый или публичный ключ), другой – для расшифрования (тайный ключ). Отметим, что указанная пара ключей принадлежит получателю зашифрованного сообщения.

Определение 1. Односторонней функцией (one-way function) называется математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, т. е., зная х, легко вычислить f(x), но по известному f(x) трудно найти подходящее значение x.

Определение 2. Ранцевый (рюкзачный) вектор S = (s1, . . ., sz) – это упорядоченный набор из z, z ≥ 3, различных натуральных чисел si. Входом задачи ранце (рюкзаке) называем пару (S, S), где S – рюкзачный вектор, а S – натуральное число. Решением для входа (S, S) будет такое подмножество из S, сумма элементов которого равняется S.

Иными словами число (меньшее, чем произведение нескольких простых чисел) однозначно определяется своими вычетами по модулю от этих простых чисел. Китайской теоремой об остатках можно воспользоваться для решения полной системы уравнений в том случае, если известно разложение числа N на простые множители

Трудный для укладки ранец применяется в качестве открытого ключа е, который легко использовать для зашифрования, но невозможно – для расшифрования. В качестве закрытого ключа d применяется легкий для укладки ранец, который предоставляет простой способ расшифрования сообщения.

В качестве закрытого ключа d (легкого для укладки ранца) используется сверхвозрастающая последовательность, состоящая из z элементов.

Определение 3. Сверхвозрастающей называется последовательность, в которой каждый последующий член больше суммы всех предыдущих.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать приложение для генерации сверхвозрастающей последовательности.

В связи с поставленными требованиями было разработано приложение на основе встроенного класса System.Numerics c его типом данных BigInteger в C#.

Пример генерации сверхвозрастающей последовательности:

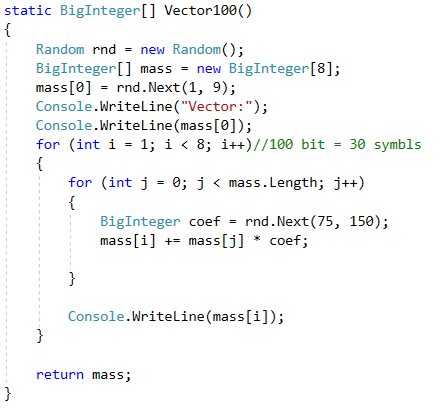


Рисунок 2.1 – Генерация сверхвозрастающей последовательности

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по асимметричных шифрам. А также, разработал приложение для шифрации/дешифрации по алгоритму укладки ранца.