МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе №6

Исследование потоковых шифров

Выполнил студент: Плюто Э. В.

ФИТ 3 курса, 5 группа

Проверил: Савельева М. Г.

Минск 2024

**Практическое задание:**

**1)** Разработать авторское приложение, которое должно реализовывать генерацию ПСП. Алгоритм генерации ПСП: линейный конгруэнтный генератор, параметры: *а* = 421, *с* = 1663, *n* = 7875.

Реализация генератора представлена на листинге 1.

|  |
| --- |
| public static void LinearCongruentialGenerator(int x, int x1)  {  int a = 421, c = 1663, n = 7875;  x1 = (a \* x1 + c) % n;  if (x1 == x)  return;  else  {  Console.WriteLine("Сгенерированное число: " + x1);  LinearCongruentialGenerator(x, x1);  }  } |

Листинг 1 – Линейный конгруэнтный генератор

Результат выполнения представлен на рисунке 1.

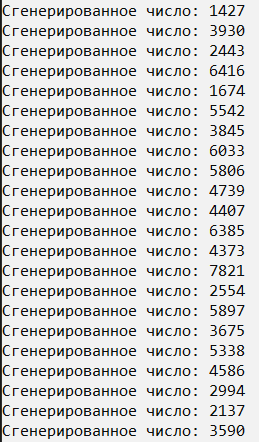


Рисунок 1 – Результат функции

**2)** Разработать авторское приложение, которое должно реализовывать генерацию ПСП. Алгоритм генерации ПСП: RC4, параметры: *n* = 8, ключ: 13, 19, 90, 92, 240.

Реализация алгоритма представлена на листинге 2.

|  |
| --- |
| public static byte[] RC4(byte[] input)  {  byte[] S = new byte[256];  for (int k = 0; k < 256; k++)  S[k] = (byte)k;  int j = 0;  for (int k = 0; k < 256; k++)  {  j = (j + S[k] + key[k % key.Length]) % 256;  Swap(S, k, j);  }  int i = 0;  j = 0;  byte[] output = new byte[input.Length];  for (int k = 0; k < input.Length; k++)  {  i = (i + 1) % 256;  j = (j + S[i]) % 256;  Swap(S, i, j);  output[k] = (byte)(input[k] ^ S[(S[i] + S[j]) % 256]);  }  return output;  } |

Листинг 2 – Реализация алгоритма RC4

Результат выполнения приложения представлен на рисунке 2.

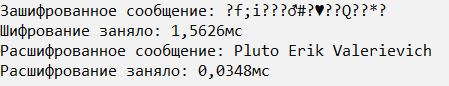


Рисунок 2 – Результат шифрования и расшифрования сообщения

Время выполнения шифрования и расшифрования сообщения представлено ниже.

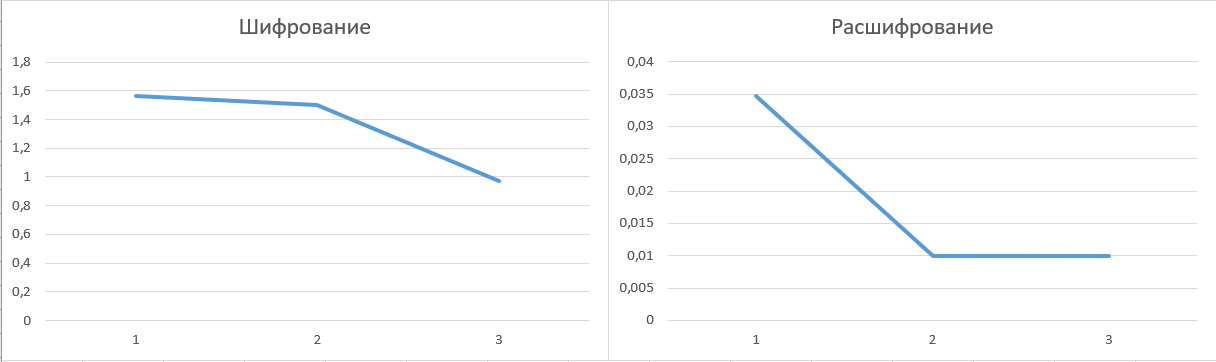


Рисунок 3 – Время выполнения шифрования и расшифрования

**Вывод:**

Были приобретены практические навыки разработки и использования приложений для реализации потоковых шифров. Были реализованы алгоритм генерации ПСП (линейный конгруэнтный генератор) и потоковый шифр с переменным размером ключа RC4. Также было замерено время выполнения шифрования и расшифрования, а также построен соответствующий график.