Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 9»**

“ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Сапегина Екатерина Игоревна,

Вариант 11 (1)

Минск 2023

***Цель:*** изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров.

***Задачи:***

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров.

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.

3. Выполнить анализ криптостойкости асимметричных шифров.

4. Оценить скорость зашифрования/расшифрования реализованных шифров. 5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

***Практическая часть:***

1. Разработать авторское оконное приложение в соответствии с

целью лабораторной работы. При этом можно воспользоваться доступными библиотеками либо программными кодами.

В основе вычислений – кодировочные таблицы Base64 и ASCII.

Приложение должно реализовывать следующие операции:

• генерация сверх возрастающей последовательности (тайного

ключа); старший член последовательности – 100-битное число;

в простейшем случае принимается z = 6 (для кодировки Base64)

и z = 8 (для кодировки ASCII);

• вычисление нормальной последовательности (открытого ключа);

• зашифрование сообщения, состоящего из собственных фамилии, имени и отчества;

• расшифрование сообщения;

• оценка времени выполнения операций зашифрования и расшифрования.

***Реализация:***

|  |
| --- |
| class AsymCrypt  {  public int[] Generate(int z)  {  Random rnd = new Random();  int[] k = new int[z];  int sum = 0;  for (int i = 0; i < z; i++)  {  k[i] = rnd.Next(sum, sum + 23);  sum += k[i];  }  return k;  }  public int[] getNorm(int[] d, int a, int n, int z)  {  int[] e = new int[z];  for (int i = 0; i < z; i++)  {  e[i] = (d[i] \* a) % n;  }  return e;  }  // Зашифрование сообщения  public int[] encode(int[] e, string M, int z)  {  int j = 0;  int[] result = new int[M.Length];  int total = 0;  foreach (char Mi in M)  {  total = 0;  string Mi2 = '0' + GetBytes(Mi.ToString()); //110010    for (int i = 0; i < Mi2.Length; i++)  {  if (Mi2[i] == '1') total += e[i];  }  result[j] = total;  j++;  }  return result;  }  //Расшифрование сообщения: Si=5, 5-3=2; 2-2=0; mi=1100000  public string decode(int[] d, int Si, int z)  {  string res = "";  string res2 = "";  for (int i = z; i > 0; i--)  {  if (Si >= d[i - 1])  {  res += '1';  Si = Si - d[i - 1];  }  else  {  res += '0';  }  }  for (int i = res.Length - 1; i > -1; i--)  {  res2 += res[i];  }  return res2;  }  public int a\_1(int a, int n)  {  int res = 0;  for (int i = 0; i < 10000; i++)  {  if (((a \* i) % n) == 1) return (i);  }  return (res);  }  public string Str(int[] a)  {  string res = "";  foreach (int x in a)  {  res += x.ToString() + "; ";  }  return res;  }  public string GetBytes(String str)  {  String strB = "";  for (int i = 0; i < str.Length; i++)  {  strB += Convert.ToString((int)str[i], 2);  }  return strB;  }  public int getN(int sum)  {  return sum + 1;  }  public int getA(int n)  {  Random rnd = new Random();  while (true)  {  int a = rnd.Next(1, 1000000);  if (Evklid(a, n) == 1)  {  return a;  }  }  }  public static int Evklid(int a, int b)  {  while (a != b)  {  if (a > b) a -= b;  else b -= a;  }  return a;  }  } |

***Результат:***

