Шапка Денис

Лабораторна робота 1 Хешування

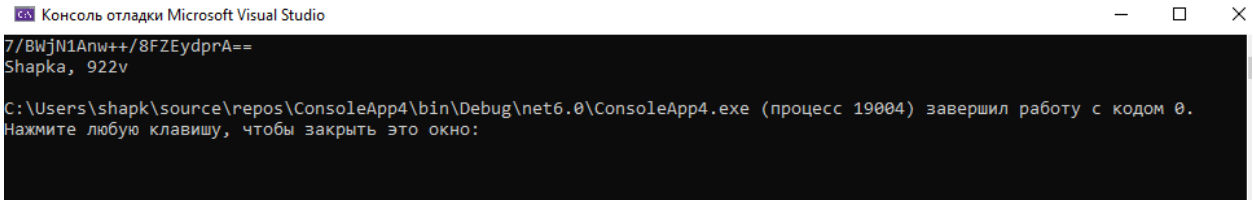
Завдання Дослідити існуючі механізми гешування. Реалізувати алгоритм гешування SHA (будь-якої версії).

Мета Дослідити принципи роботи гешування.

Текст програми

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Security.Cryptography;
using System.IO;

namespace Lab1
{
   class Program
   {
      public static string Shifrovka(string ishText, string pass,
            string sol = "Kitty", string cryptographicAlgorithm = "SHA1",
            int passIter = 2, string initVec = "a8doSuDitOz1hZe#",
            int keySize = 256)
      {
         byte[] initVecB = Encoding.ASCII.GetBytes(initVec);
         byte[] solB = Encoding.ASCII.GetBytes(sol);
         byte[] ishTextB = Encoding.UTF8.GetBytes(ishText);

         PasswordDeriveBytes derivPass = new PasswordDeriveBytes(pass, solB, cryptographicAlgorithm,
passIter);
         byte[] keyBytes = derivPass.GetBytes(keySize / 8);
         RijndaelManaged symmK = new RijndaelManaged();
         symmK.Mode = CipherMode.CBC;
```

```
            byte[] cipherTextBytes = null;


            using (ICryptoTransform encryptor = symmK.CreateEncryptor(keyBytes, initVecB))
            {
               using (MemoryStream memStream = new MemoryStream())
               {
                  using (CryptoStream cryptoStream = new CryptoStream(memStream, encryptor,
CryptoStreamMode.Write))
                  {
                     cryptoStream.Write(ishTextB, 0, ishTextB.Length);
                     cryptoStream.FlushFinalBlock();
                     cipherTextBytes = memStream.ToArray();
                     memStream.Close();
                     cryptoStream.Close();
                  }
               }
            }


            symmK.Clear();
            return Convert.ToBase64String(cipherTextBytes);
         }



         static void Main(string[] args)
         {


            String gg = Shifrovka("Shapka, 922v", "пароль");
            Console.WriteLine(gg);
            Console.WriteLine("Shapka, 922v");
         }
      }
   }
```


Консоль отладки Microsoft Visual Studio
7/BWjN1Anw++/8FZEydprA==
Shapka, 922v
C:\Users\shapk\source\repos\ConsoleApp4\bin\Debug\net6.0\ConsoleApp4.exe (процесс 19004) завершил работу с кодом 0.
Нажмите любую клавишу, чтобы закрыть это окно: