Министерство образования Республики Беларусь

Учреждение образования

“Белорусский государственный университет информатики и радиоэлектроники”

Кафедра инженерной психологии и эргономики

Практическая работа №3

«Шифрование, дешифрование информации с применением криптографических алгоритмов гаммирование»

Проверил: Выполнила:

Давыдович К.И. ст. гр.910903 Неверова А.П.

Минск 2022

**Цель работы:** используя алгоритм шифрования гаммирования зашифровать текст с заданным ключом и расшифровать полученный шифр.

**Задание №1:**

Открытый текст: secret.

Ключ: key.

Результат шифрования: "\0\0\r"

**Код программы:**

using System.Text;  
  
namespace CaesarsSipher;  
  
public static class Gamma  
{  
 private const string **Text** = "secret";  
 private const string **Key** = "key";  
  
 private static byte[] GetAsciiBytes(string value)  
 {  
 return Encoding.ASCII.GetBytes(value);  
 }  
  
 private static string GetValueByAsciiBytes(byte[] bytes)  
 {  
 return Encoding.ASCII.GetString(bytes);  
 }  
   
 private static string GetValidKey(string key, int length)  
 {  
 if (key.Length >= length)  
 {  
 return key;  
 }  
 var newKey = key;  
 for(var i = 0; i<length - key.Length; i++)  
 {  
 newKey += key[i % key.Length];  
 }  
  
 return newKey;  
 }  
  
 private static byte[] GetSipher(byte[] text, byte[] key)  
 {  
 var sipher = new List<byte>();  
 for (var i = 0; i < text.Length; i++)  
 {  
 sipher.Add((byte)(text[i]^key[i]));  
 }  
  
 return sipher.ToArray();  
 }  
  
 public static void ShowWork()  
 {  
 var textInBytes = GetAsciiBytes(**Text**);  
 var keyInBytes = GetAsciiBytes(GetValidKey(**Key**, **Text**.Length));  
 var sipher = GetSipher(textInBytes, keyInBytes);  
 Console.WriteLine($"Real text: {**Text**}");  
 Console.WriteLine($"Key: {**Key**}");  
 Console.WriteLine($"Sipher: {GetValueByAsciiBytes(sipher)}");  
 var realText = GetValueByAsciiBytes(GetSipher(sipher, GetAsciiBytes(GetValidKey(**Key**, **Text**.Length))));  
   
 Console.WriteLine($"Real text: {realText}");  
 }  
}

**Вывод:** зашифровала текст, используя алгоритм гаммирования. Расшифровала полученный шифротекст.