Протокол самостоятельной работы

По Теории Защиты Информации

На тему: Шифр Цезаря

Выполнил студент К17.1

Шишелов Владимир

**Шифр Цезаря**

Историческим примером шифра замены является шифр Цезаря (1 век до н. .),  описанный  историком  Древнего  Рима   Светонием.  Гай  Юлий  Цезарь использовал  в  своей  переписке  шифр  собственного  изобретения.  Идея  этого шифра состояла в следующем. Выписывался алфавит в обычном виде, а затем  под  ним  выписывался  тот  же  алфавит,  но  со  сдвигом  на 3  буквы  вправо.

При зашифровке буква А заменялась буквой Г, буква Б заменялась на Д и так далее. Ключом  в  шифре  Цезаря  является величина сдвига нижней строки алфавита. В нашем случае – это число 3.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

https://lh4.googleusercontent.com/05PC0eREj4DMUGGvqQuylji6XN83dJcqr5FKZHVwHtxMh6zweb5ttkcgJ5TmNLrb2OoMZ7XILZJY8UWqEaQCmf-OEz7vLgXPdWWXj1TdZErnQ0AA-HWbDHn6vL0abB7jc5jeTCY

https://lh4.googleusercontent.com/Hdw-9eQqkJ6mQeTmmqryvYN2S4dv2O9dFuwhc8WhIvHQKIEV7_P28kxX1MC5PuwaDlRBq4GpLXa7nejopNmGmiN1df3pdvGwslt1IdH41c7Dsy33xHi2RCNZ2ZCKNZMdPlrZv88

где https://lh6.googleusercontent.com/YaiApQw-q2saHxQvoAuJuT854twZwbxW21qvIDZpntHSOnKIJar_U5rzRRf8oHSr5pMPUiqEQ1lX9jdgWQPUE_LtwJ1oWxek8xkp2zdR8AHebD1v28vO3YcRBaLbbw421DNAfR8 — символ открытого текста, https://lh6.googleusercontent.com/9BrroCdoFTNW6QoldYXEhK_qAell-ggePAP98_eye35RUdcb73l5lz4m1NQL1m-q6wsh0_o-Sb_ZKDQ2DER8OGvJOtCRvsQw8iMfjhSPzDGm0ltQfhidUSPmh7RIeRekpAGDbKM — символ шифрованного текста, https://lh6.googleusercontent.com/TK-yI7IzJOdVVolWt675hzy5woe0Hj3qwWbImy_Y-LUOeyVv6gWa8zBjlNltA_ij75rhP496UzdDICBDnbZr1wdZYhZ0GB5MeCwK8X4RpD6woPvuB53pTU6kK1Yp-5y4A-1R7cM — мощность алфавита, а https://lh5.googleusercontent.com/Ge_Py73YVTTMeZX0fWu8jE5i8WcrLTiXL52XJip4G2oZS9cfBYpUGPhjfEgk8p1q6CBQtsd8d6N634Zgek9ciI7XjYC0lbktTB-h2y15fnm8ZRnbxU6D5OiKWuxrhNdMrM_ZH6M — ключ.

Условием  для  успешной  реализации  этого  метода  является  совпадение размера  множеств  открытого  текста  и  шифротекста.  Это  условие  в современных криптосистемах называется гомоморфизмом.

Позднее  были предложены многочисленные модификации  этого шифра, которые  были  направлены  на  повышение  криптостойкости (устойчивости  к дешифрованию).

Более эффективны обобщения подстановки Цезаря – шифр Хилла и шифр Плэйфер. Они основаны на подстановке не отдельных символов, а  двуграмм (шифр  Плэйфер)  и n-грамм (шифр  Хилла).  При  более  высокой криптостойкости  они  значительно  сложнее  для  реализации  и  требуют достаточно большого количества ключевой информации.

Шифр, называемый шифром Гронсфельда, состоит в модификации шифра  Цезаря числовым ключом. Для этого под сообщением пишут числовойключ.  При  шифровании  сдвиг  происходит  не  на  постоянную  величину,  а  на цифру, указанную под шифруемой буквой в ключе.

**Реализация Шифра на языке программирования С#.**

public class CaesarCipher

{

//символы русской азбуки

const string alfabet = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";

private string CodeEncode(string text, int k)

{

//добавляем в алфавит маленькие буквы

var fullAlfabet = alfabet + alfabet.ToLower();

var letterQty = fullAlfabet.Length;

var retVal = "";

for (int i = 0; i < text.Length; i++)

{

var c = text[i];

var index = fullAlfabet.IndexOf(c);

if (index < 0)

{

//если символ не найден, то добавляем его в неизменном виде

retVal += c.ToString();

}

else

{

var codeIndex = (letterQty + index + k) % letterQty;

retVal += fullAlfabet[codeIndex];

}

}

return retVal;

}

//шифрование текста

public string Encrypt(string plainMessage, int key)

=> CodeEncode(plainMessage, key);

//дешифрование текста

public string Decrypt(string encryptedMessage, int key)

=> CodeEncode(encryptedMessage, -key);

}

class Program

{

static void Main(string[] args)

{

var cipher = new CaesarCipher();

Console.Write("Введите текст: ");

var message = Console.ReadLine();

Console.Write("Введите ключ: ");

var secretKey = Convert.ToInt32(Console.ReadLine());

var encryptedText = cipher.Encrypt(message, secretKey);

Console.WriteLine("Зашифрованное сообщение: {0}", encryptedText);

Console.WriteLine("Расшифрованное сообщение: {0}", cipher.Decrypt(encryptedText, secretKey));

Console.ReadLine();

}

}