Протокол самостоятельной работы

По Теории Защиты Информации

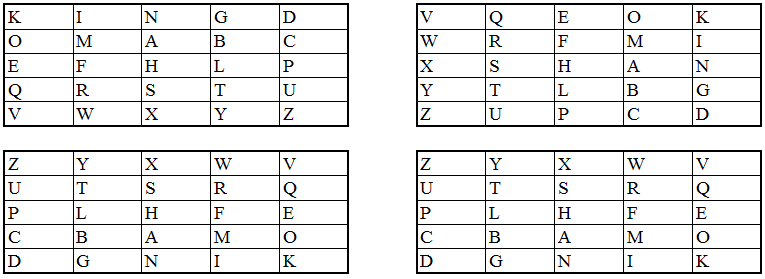
На тему: Шифр Квадрата

Выполнил студент К17.1

Шишелов Владимир

**Шифр четырех квадратов**

Для шифрования текста создаются четыре квадрата (размер зависит от мощности алфавита) с произвольно заполненными в них буквами алфавита. Данные квадраты также располагаются в виде квадрата.

****

Данный шифр является представителем биграммных шифров. Бигра́ммный шифр — это криптографический алгоритм, который предназначен для шифрования групп из двух букв (биграмм).

Алгоритм шифрования:

1. Биграмма находилась в двух, расположенных наискось, таблицах – первая буква из первой таблицы, вторая – из второй.
2. На их пересечении выбирались буквы из двух оставшихся таблиц. Выбор происходит с верхней таблицы.
3. Полученная таким образом биграмма является шифр-текстом.

Например:  SF-->LA.

Важным замечанием при использовании этого шифра является то, что количество символов слова должно быть кратно двум. Если это правило не соблюдается, то в конец добавляю «незначащую» букву. Расшифрование текста происходит в обратном порядке.

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

private static string FourScCipher(string input, string key, bool encipher)

{

string retVal = string.Empty;

char[,] keySquare = GenerateKeySquare(key);

string tempInput = RemoveOtherChars(input);

int e = encipher ? 1 : -1;

if ((tempInput.Length % 2) != 0)

tempInput += "X";

for (int i = 0; i < tempInput.Length; i += 2)

{

int row1 = 0;

int col1 = 0;

int row2 = 0;

int col2 = 0;

GetPosition(ref keySquare, char.ToUpper(tempInput[i]), ref row1, ref col1);

GetPosition(ref keySquare, char.ToUpper(tempInput[i + 1]), ref row2, ref col2);

if (row1 == row2 && col1 == col2)

{

retVal += new string(SameRowColumn(ref keySquare, row1, col1, e));

}

else if (row1 == row2)

{

retVal += new string(SameRow(ref keySquare, row1, col1, col2, e));

}

else if(col1 == col2)

{

retVal += new string(SameColumn(ref keySquare, col1, row1, row2, e));

}

else

{

retVal += new string(DifferentRowColumn(ref keySquare, row1, col1, row2, col2));

}

}

retVal = AdjustOutput(input, retVal);

return retVal;

}

public static string Encipher(string input, string key)

{

return FourScCipher(input, key, true);

}

public static string Decipher(string input, string key)

{

return FourScCipher(input, key, false);

}