Протокол самостоятельной работы

По Теории Защиты Информации

На тему: Шифр Виженера

Выполнил студент К17.1

Шишелов Владимир

**Шифр Виженера**

Шифр Виженера — метод полиалфавитного [шифрования](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80) буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо в книге La cifra del. Sig. Giovan Battista Bellasо в 1553 году, однако в XIX веке получил имя [Блеза Виженера](http://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80,_%D0%91%D0%BB%D0%B5%D0%B7), французского дипломата.

Первое точное документированное описание многоалфавитного шифра было сформулированно [Леоном Баттиста Альберти](http://ru.wikipedia.org/wiki/%D0%90%D0%BB%D1%8C%D0%B1%D0%B5%D1%80%D1%82%D0%B8,_%D0%9B%D0%B5%D0%BE%D0%BD_%D0%91%D0%B0%D1%82%D1%82%D0%B8%D1%81%D1%82%D0%B0) в 1467 году, для переключения между алфавитами использовался металлический шифровальный диск. Система Альберти переключает алфавиты после нескольких зашифрованных слов. Позднее, в 1518 году, [Иоганн Трисемус](http://ru.wikipedia.org/wiki/%D0%98%D0%BE%D0%B3%D0%B0%D0%BD%D0%BD_%D0%A2%D1%80%D0%B8%D1%81%D0%B5%D0%BC%D1%83%D1%81) в своей работе «Полиграфия» изобрел tabula recta — центральный компонент шифра Виженера.

То, что сейчас известно под шифром Виженера, впервые описал Джованни Батиста Беллазо в своей книге La cifra del. Sig. Giovan Battista Bellasо. Он использовал идею tabula recta Трисемуса, но добавил ключ для переключения алфавитов шифра через каждую букву.

[Блез Виженер](http://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80,_%D0%91%D0%BB%D0%B5%D0%B7) представил своё описание простого, но стойкого шифра перед комиссией [Генриха III](http://ru.wikipedia.org/wiki/%D0%93%D0%B5%D0%BD%D1%80%D0%B8%D1%85_III_(%D0%BA%D0%BE%D1%80%D0%BE%D0%BB%D1%8C_%D0%A4%D1%80%D0%B0%D0%BD%D1%86%D0%B8%D0%B8)) во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему. Давид Кан в своей книге «Взломщики кодов» отозвался об этом осуждающе, написав, что история «проигнорировала важный факт и назвала шифр именем Виженера, несмотря на то, что он ничего не сделал для его создания».

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон ([Льюис Кэрролл](http://ru.wikipedia.org/wiki/%D0%9B%D1%8C%D1%8E%D0%B8%D1%81_%D0%9A%D1%8D%D1%80%D1%80%D0%BE%D0%BB%D0%BB)) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр» [англ.](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) The Alphabet Cipher, опубликованной в детском журнале в 1868 году. В 1917 году [Scientific American](http://ru.wikipedia.org/wiki/Scientific_American) также отозвался о шифре Виженера, как о неподдающемся взлому. Это представление было опровергнуто после того, как [Касиски](http://ru.wikipedia.org/wiki/%D0%9A%D0%B0%D1%81%D0%B8%D1%81%D0%BA%D0%B8,_%D0%A4%D1%80%D0%B8%D0%B4%D1%80%D0%B8%D1%85) полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

Шифр Виженера достаточно прост для использования в полевых условиях, особенно если применяются шифровальные диски. Например, «конфедераты» использовали медный шифровальный диск для шифра Виженера в ходе [Гражданской войны](http://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%D1%81%D0%BA%D0%B0%D1%8F_%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0_%D0%B2_%D0%A1%D0%A8%D0%90). Послания Конфедерации были далеки от секретных, и их противники регулярно взламывали сообщения. Во время войны командование Конфедерации полагалось на три ключевых словосочетания: «Manchester Bluff», «Complete Victory» и — так как война подходила к концу — «Come Retribution».

[Гилберт Вернам](http://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%BB%D0%B1%D0%B5%D1%80%D1%82_%D0%92%D0%B5%D1%80%D0%BD%D0%B0%D0%BC) попытался улучшить взломанный шифр (он получил название шифр Вернама-Виженера в 1918 году), но, несмотря на его усовершенствования, шифр так и остался уязвимым к [криптоанализу](http://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7). Однако работа Вернама в конечном итоге всё же привела к получению шифра, который действительно невозможно взломать.

В [шифре Цезаря](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет вид:

**ATTACKATDAWN**

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

**LEMONLEMONLE**

Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

Исходный текст:           **ATTACKATDAWN**

Ключ:                            **LEMONLEMONLE**

Зашифрованный текст: **LXFOPVEFRNHR**

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если буквы A-Z соответствуют числам 0-25, то шифрование Виженера можно записать в виде формулы:

https://lh3.googleusercontent.com/xeQbUTh66CVA-UaMGsBqJ4IApdKv5wwORZXzGNZsjB3iMWwqWQOhFk3foow1Vxs3dbhsNJ2ESO7M5R56a0BCGxttKNUVij3Gcw0r75sYQMP1RLiX8wwdb3HhqOObu1Db02UTUbY

Расшифровка:

https://lh6.googleusercontent.com/97yqkiBR6WMg1Mzq_dqYBcQa-hM-oh7WT_w2RcqjIee2xBKKvH2uwzGCKedw8D2ECRyebe8BoZAUFu_3URRyiVs35Y2HJDQmaiZSY5tSr4nKQ_YIhOl_8tHvOuW9mmiSBB7ZNgo

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

public class VigenereCipher

{

const string defaultAlphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";

readonly string letters;

public VigenereCipher(string alphabet = null)

{

letters = string.IsNullOrEmpty(alphabet) ? defaultAlphabet : alphabet;

}

//генерация повторяющегося пароля

private string GetRepeatKey(string s, int n)

{

var p = s;

while (p.Length < n)

{

p += p;

}

return p.Substring(0, n);

}

private string Vigenere(string text, string password, bool encrypting = true)

{

var gamma = GetRepeatKey(password, text.Length);

var retValue = "";

var q = letters.Length;

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

{

var letterIndex = letters.IndexOf(text[i]);

var codeIndex = letters.IndexOf(gamma[i]);

if (letterIndex < 0)

{

//если буква не найдена, добавляем её в исходном виде

retValue += text[i].ToString();

}

else

{

retValue += letters[(q + letterIndex + ((encrypting ? 1 : -1) \* codeIndex)) % q].ToString();

}

}

return retValue;

}

//шифрование текста

public string Encrypt(string plainMessage, string password)

=> Vigenere(plainMessage, password);

//дешифрование текста

public string Decrypt(string encryptedMessage, string password)

=> Vigenere(encryptedMessage, password, false);

}

class Program

{

static void Main(string[] args)

{

//передаем в конструктор класса буквы русского алфавита

var cipher = new VigenereCipher("АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ");

Console.Write("Введите текст: ");

var inputText = Console.ReadLine().ToUpper();

Console.Write("Введите ключ: ");

var password = Console.ReadLine().ToUpper();

var encryptedText = cipher.Encrypt(inputText, password);

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

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

Console.ReadLine();

}

}