

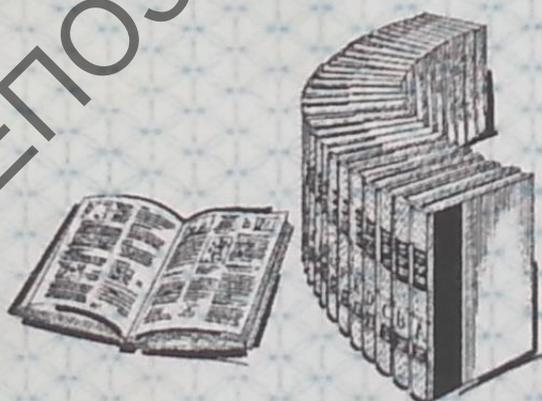
*КРИПТОГРАФИЯ. АЛГОРИТМЫ
ШИФРОВАНИЯ ВИЖЕНЕРА, ЕГО
РЕАЛИЗАЦИЯ В DELFI*

Александр Францкевич

Frantskevich@live.ru



СТУДЕНЧЕСКАЯ НАУКА КАК ФАКТОР ЛИЧНОСТНОГО И ПРОФЕССИОНАЛЬНОГО РАЗВИТИЯ БУДУЩЕГО СПЕЦИАЛИСТА



Материалы VII студенческой
научно-практической конференции

Шифр Виженера представляет собой усовершенствованную многоалфавитную систему шифрования. Идея шифра состоит в использовании в качестве ключа (кодированное слово) текста самого сообщения (открытого – не зашифрованного) или же зашифрованного текста (закрытого). Кроме того, для усиления стойкости шифра, в качестве первого символа ключа берется случайным образом буква из алфавита. Авторами этой идеи являются Джероламо Кардано и собственно сам Блез де Вижнер. Данный шифр также имеет другое название «шифр самоключа». Этот шифр Вижнер описал в своей книге «Трактат о шифрах»: «В простейшем случае за основу бралась таблица Тритемия. В последствии она получила название «таблица Виженера».

Отметим, что в общем случае таблица Виженера состоит из алфавита, циклически сдвинутого на один символ влево, однако, возможны и другие перестановки – это на Ваше усмотрение. Кроме того, первая строка может представлять собой алфавит, случайным образом перемешанный.

Процесс шифрования выглядит следующим образом: открытый текст (который надо зашифровать) записывается в строку без пробелов. Далее необходимо определить ключ. Вижнер предлагал в качестве ключа использовать сам открытый текст, с добавлением к началу ключа символ, выбранный случайным образом. Отметим, что не обязательно следовать установленному правилу

создателя шифра. В качестве ключа вполне возможно использовать и любую другую последовательность символов длиной равной длине открытого текста.

После всего сделанного, для получения шифр-текста (криптограмма) берем первый символ открытого текста в качестве указателя строки в Таблице Виженера, а стоящую под ним букву – в качестве столбца. На пересечении этой пары из таблицы выписываем символ шифр-текста. Далее повторяем эти действия для всех оставшихся символов. Для примера рассмотрим шифрование открытого текста – «яблочный джем». В качестве ключа будем использовать сам открытый текст с добавлением в начала случайного символа – у нас это вышло «щ» (ключ может быть образован иным способом, к примеру просто перемешанный случайным образом открытый текст – «ляйычнбо жемд»). Но ключ должен быть известен получателю шифра, то есть известна схема перемешивания открытого текста для того, чтобы он мог расшифровать криптограмму. Так, теперь записываем открытый текст в строку без пробелов, а под ней также записываем ключ. Получаем:

открытый текст: я б л о ч н ы й д ж е м

ключ: щ я б л о ч н ы й д ж е

шифр-текст: ш а м щ е д й д н к л с

Для того чтобы восстановить (расшифровать) открытый текст, необходимо знать шифр-текст и ключ. Далее берем первую букву ключа определяем соответствующий ей столбец в Таблице Виженера и пробегаемся по нему сверху вниз пока не встретим первый символ шифр-текста. Как только встретили нужный символ, выписываем букву указывающую на эту строку – таким образом мы получаем первый символ открытого текста. Прodelываем те же действия для оставшихся символов ключа и шифр-текста.

Шифр Виженера был незаслуженно забыт на долгое время. И многие по сей день под этим шифром понимают самый простой вариант с коротким ключевым словом и с таблицей, состоящей из обычных алфавитов.

А теперь рассмотрим программную реализацию шифра Виженера на Delphi.

Для начала нам необходимо сгенерировать саму таблицу Виженера. Для этого необходимо объявить следующие глобальные переменные:

```
mas_alf: array[1..32] of char =  
( 'A', 'Б', 'В', 'Г', 'Д', 'Е', 'Ж', 'З', 'И', 'Й', 'К', 'Л', 'М', 'Н', 'О', 'П', 'Р', 'С', 'Т', 'У', 'Ф', 'Х', 'Ц', 'Ч', 'Ш', 'Щ', 'Ъ', 'Ы', 'Ь', 'Э', 'Ю', 'Я' );  
tab_Vig: array[1..32, 1..32] of Char;
```

Ну а теперь напишем код генерации таблицы:

```
var i, j, k, n: integer;  
begin k:=0; n:=k; for i:=Ord('A')-191 to Ord('Я')-191 do  
begin k:=n+1; for j:=Ord('A')-191 to Ord('Я')-191 do  
begin if k = 33 then k:=1; tab_vig[i][j]:=mas_alf[k]; k:=k+1; end; n:=n+1; end;  
end;
```

Таблица есть и можно смело приступать к реализации процедуры шифрования. Смотрим:

```
Var key : array [0..255] of Char; s:char;k:Boolean;  
length_key,length_text,i,j,c,stroka,stolbec: integer;  
begin Label5.Caption:=""; Memo2.Clear; length_key:=Edit1.GetTextLen;
```

```

Edit1.GetTextBuf(key,sizeof(key)); length_text:=Memo1.GetTextLen;
//выводим таблицу Виженера
for i:=Ord('A')-191 to Ord('Я')-191 do
begin for j:=Ord('A')-191 to Ord('Я')-191 do
begin Label5.Caption:= Label5.Caption +' '+ tab_Vig[i][j]; end;
Label5.Caption := Label5.Caption + #13+#10; end;
//приступаем к процессу шифрования
j:=1; c:=0; k:=false; Memo2.Lines.Add('Зашифрованный текст:');
Memo2.Lines.Add('-----');
for i:= 0 to Memo1.Lines.Count-1 do
begin s:=Memo1.Lines[i][j]; if ((s <> #0) or (s <> #13)) then while k = false do
begin if Ord(key[c])>223 then stolbec:=Ord(key[c])-32-191 else
stolbec:=Ord(s)-191; if Ord(s)>223 then
stroka:=Ord(s)-32-191 else stroka:=Ord(s)-191;
Memo2.Text:=Memo2.Text+tab_Vig[stroka][stolbec];
if(c < length_key-1)then c:=c+1 else c:=0; j:=j+1; s:=Memo1.Lines[i][j];
if(s = #0) then k:=true; end; k:=false; j:=1; end;
Memo2.Lines.Add('-----');end;

```

Так как шифрование реализовано, значит пора рассмотреть процедуру расшифровки. Смотрим:

```

var key : array [0..255] of Char; s:char; k:Boolean;
length_key,length_text,i,j,c,stroka,stolbec,q: integer;
begin Label5.Caption:=""; Memo2.Clear; length_key:=Edit1.GetTextLen;
Edit1.GetTextBuf(key,sizeof(key)); length_text:=Memo1.GetTextLen;
j:=1; c:=0; k:=false; Memo2.Lines.Add('Расшифрованный текст:');
Memo2.Lines.Add('-----');
for i:= 0 to Memo1.Lines.Count-1 do
begin if Ord(Memo1.Lines[i][j])>223 then c:=Ord(Memo1.Lines[i][j])-32-191
else s:=Ord(Memo1.Lines[i][j])-191; s:=Memo1.Lines[i][j];
if ((s <> #0) or (s <> #13)) then while k = false do
begin if Ord(key[c])>223 then stolbec:=Ord(key[c])-32-191
else stolbec:=Ord(s)-191; for q:=1 to 32 do
begin if tab_Vig[q][stolbec]=s then
begin Memo2.Text:=Memo2.Text+Chr(q+191); break; end; end;
if(c < length_key-1)then c:=c+1 else c:=0; j:=j+1; s:=Memo1.Lines[i][j];
if(s = #0) then k:=true; end; k:=false; j:=1; end;
Memo2.Lines.Add('-----');end;

```

Литература

1. Конхейм, А.Г. Основы криптографии / А.Г. Конхейм. – М.: Радио и связь, 1987.
2. Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / Б.Я. Рябко, А.Н. Фионов. – М.: Научный мир, 2004.

Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный педагогический университет
имени Максима Танка»

**СТУДЕНЧЕСКАЯ НАУКА
КАК ФАКТОР ЛИЧНОСТНОГО
И ПРОФЕССИОНАЛЬНОГО РАЗВИТИЯ
БУДУЩЕГО СПЕЦИАЛИСТА**

Материалы

VII студенческой научно-практической конференции

г. Минск, 29 апреля 2011 г.

Минск 2011

Печатается по решению редакционно-издательского совета БГПУ

Редколлегия:

доктор политических наук, проректор по научной работе БГПУ *В.В. Бущик*;
доктор технических наук, профессор *В.М. Добрянский*;
доктор филологических наук, профессор *В.Д. Стариченок*;
доктор физико-математических наук, профессор *И.С. Ташлыков*;
доктор педагогических наук, профессор *В.В. Шлыков*;
кандидат педагогических наук, доцент *С.Е. Гайдукевич*;
кандидат физико-математических наук, доцент *В.И. Януть*

Рецензенты:

кандидат филологических наук, доцент *Т.В. Багуня*;
кандидат биологических наук, доцент *В.Ф. Кулеш*;
кандидат социологических наук, доцент *Д.И. Наумов*;
кандидат педагогических наук, доцент *Н.К. Пещенко*;
кандидат педагогических наук, доцент *Л.Н. Тимашкова*;
кандидат психологических наук, доцент *В.А. Хрипович*

РЕПОЗИТОРИЙ БГПУ

С88 **Студенческая наука как фактор личностного и профессионального развития будущего специалиста:** материалы VII студ. науч.-практ. конф., г. Минск, 29 апр. 2011 г. / Бел. гос. пед. ун-т им. М. Танка; редкол. В.В. Бущик, В.М. Добрянский, В.Д. Стариченок и др. – Минск : БГПУ, 2011. – 220 с.
ISBN 978-985-501-976-4.

В сборнике представлены материалы исследований студентов БГПУ, посвященные проблемам педагогических, психологических, гуманитарных и естественно-научных дисциплин. Адресуется преподавателям, магистрантам и студентам вузов.

Карневич О.Н. Формирование математической компетентности учащихся при изучении функциональной линии на второй ступени общего среднего образования	153
Ковгореня Л.В. Задачи на применение производной как средство развития творческих способностей у учащихся	155
Курапова И.И. Моделирование в школьном курсе математики	157
Кутьш А.З. Оценка сложности алгоритмов решения японских кроссвордов	159
Кураш Е.А., Галамака В.А. Запись объемных голограмм в активированном красителем желатиновом геле	161
Мергурьев А.Н., Маньло А.И. Моделирование физических явлений в Интернет: технологии FLASH и HTML5	162
Олешкевич П.А. Принцип системности как средство систематизации и обогащения знаний учащихся при решении задач на построение в пространстве	163
Скородово О.З., Кравченко И.Н. Построение интегрального представления решений одной системы дифференциальных уравнений	165
Терешко О.А. Алгоритмический подход при решении текстовых задач	167
Терпицкая Е.Ю. Теоретические основы практических достижений учителей-новаторов	169
Харитончик И.Н. Спонтанная поляризация, коэрцитивные и смещающие поля	171
Швайко Т.М. Интеграция разделов школьной математики при решении геометрических задач на экстремумы	173
Фесенко О.А., Шенетуха Т.Ю. Фракталы в физике природных явлений	175
Францкевич А.А. Криптография. Алгоритмы шифрования Виженера, его реализация в Delphi	176
Шимкович Т.Г. Решение задач с параметрами как средство развития творческого потенциала учащихся 10–11 классов	179
Шпаковская Н.Г. Методические особенности организации повторения начал стереометрии	180
Щелкунова В.А. Пути повышения качества и эффективности уроков математики в начальной школе	182
Яковенко Ю.С. Смачиваемость поверхности фольг алюминиевых сплавов, получаемых сверхбыстрой закалкой из расплава	184
Яскевич А.В. Самостоятельная работа на уроках математики в начальных классах	185
Ящук Д.В. Применение личностно ориентированной технологии на уроках физики	187