ПОД- СЕКЦИЯ 6. Математика.

Шевцов А.Н.,
кандидат технических наук, доцент кафедры «Прикладная математика»
Таразский Государственный университет им. М.Х.Дулати
Туймебаева А.Е.,
кандидат физ.-мат. наук, доцент кафедры «Прикладная математика»
Таразский Государственный университет им. М.Х.Дулати
Шенгелбаева У.К.
студент 4 курс,
Таразский Государственный университет им. М.Х.Дулати

РАЗРАБОТКА КОДИРОВЩИКА НА DELPHI ДЛЯ АЛГОРИТМА ЭЛЬ-ГАМАЛЯ

Хотя сам алгоритм Эль-Гамаля (криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле) хорошо описан в различных источниках [1, с.1; 2, с.318], тем не менее его реализация представляет довольно большие трудности. Для его исследования, создадим кодировщик – реализующий метод Эль-Гамаля.

Для шифрования необходимо вычислить открытый и закрытый ключи, и также шифротекст:

$$(p, g, y), \quad (x) \quad (a, b).$$

Для расшифровки достаточно воспользоваться формулой:

$$M = b \cdot a^{p-1-x} \bmod p.$$

Произвольное сообщение будем разбивать на отдельные цифры и вычислять шифротекст. Разработаем алгоритм для шифрования:

code: Delphi

```
procedure TForm1.BitBtn1Click(Sender: TObject);
var    i, j: Integer;    s, sum:string;
 begin
p:=strtoint(edit1.Text);     g:=strtoint(edit2.Text);
randomize;            x:=random(p-3)+2;
st:=trunc(power(g,x));  y:=st mod p;
// (p,g,y)   //  x    //  (a,b)
randomize;            k:=random(p-4)+2;
memo2.Clear;
for i := 0 to memo1.Lines.Count - 1 do
begin
s:=memo1.Lines.Strings[i];
for j := 1 to length(s) do
begin
M:=strtoint(s[j]);
st:=trunc(power(g,k));  a:=  st mod p;
st:=trunc(power(y,k));  b:=(st*M) mod p;
memo2.Lines.Add(inttostr(a)+' '+inttostr(b));
end;  end;
```

А также для восстановления исходного сообщения:

code: Delphi

```
sum:='';
for i := 0 to memo2.Lines.Count - 1 do
begin
s:=memo2.Lines.Strings[i];
a:=strtoint(GetToken(s,' ',1));    b:=strtoint(GetToken(s,' ',2));
st:=trunc(b*power(a,p-1-x));     m:=st mod p;
sum:=sum+inttostr(m);
end;
memo3.Lines.Add(sum);
end;
```

Проверим на основе [1, с.1], как видим алгоритм рабочий и полностью восстановил сообщение (рис.1).

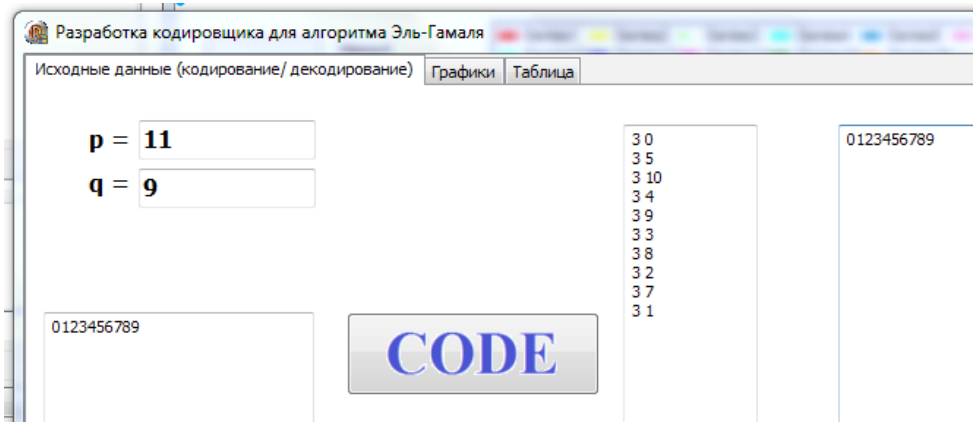

Рисунок 1 – Кодирование и декодирование сообщения.

На значения p и q, вводятся ограничения, p- простое число, а q- целое. И действительно при $p = 1$ а q – произвольное целое, меньше q, все выполняется и сообщение полностью восстанавливается. Исследуем задачу при других p. В случае q=1 наблюдаем полное восстановление для отдельных p, но при q=1,2,3,4,5 получим (табл.1-5). Получаем независимо от введенных Эль-Гамалем ограничений, плавающий процент успешного восстановления сообщений. В отдельных случаях он падает в среднем до 10% (рис.2), что недопустимо при кодировании и передачи данных, и это с учетом того, что нам был известен закрытый ключ.

Таблица 1

Процент успешного восстановления закодированных сообщений, q=1.

P	p=3	p=4	p=5	p=6	p=7	p=8	p=9	p=10
% восстановления	0	0	0	0	0	0	0	100
P	p=11	p=12	p=13	p=14	p=15	p=16	p=17	
% восстановления	100	100	100	100	100	100	100	

Таблица 2

Процент успешного восстановления закодированных сообщений, q=2.

P	p=3	p=4	p=5	p=6	p=7	p=8	p=9	p=10
% восстановления	0	0	0	0	0	0	0	0
P	p=11	p=12	p=13	p=14	p=15	p=16	p=17	
% восстановления	100	0	78-88	0	45-59	0	32-51	

Таблица 3

Процент успешного восстановления закодированных сообщений, q=3.

P	p=3	p=4	p=5	p=6	p=7	p=8	p=9	p=10
% восстановления	0	0	0	0	0	0	0	14-29
P	p=11	p=12	p=13	p=14	p=15	p=16	p=17	
% восстановления	100	0	92-98	20-31	0	16-27	16-28	

Таблица 4

Процент успешного восстановления закодированных сообщений, q=4.

P	p=3	p=4	p=5	p=6	p=7	p=8	p=9	p=10
% восстановления	0	0	0	0	0	0	0	0
P	p=11	p=12	p=13	p=14	p=15	p=16	p=17	
% восстановления	100	0	59-70	0	100	0	31-55	

Таблица 5

Процент успешного восстановления закодированных сообщений, q=5.

P	p=3	p=4	p=5	p=6	p=7	p=8	p=9	p=10
% восстановления	0	0	0	0	0	0	0	0
P	p=11	p=12	p=13	p=14	p=15	p=16	p=17	
% восстановления	100	42-60	74-85	8-16	0	12-20	14-25	

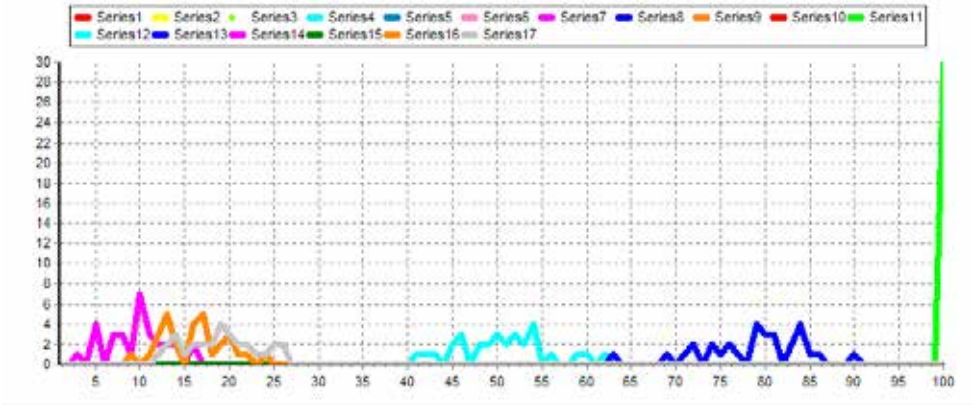

Рисунок 2 – Функция распределения, для случаев успешного восстановления данных при q=5.

Литература.

1. Схема Эль-Гамаля. Материал из Википедии — свободной энциклопедии. http://ru.wikipedia.org/wiki/%D1%F5%E5%EC%E0_ %DD%EB%FC-%C3%E0%EC%E0%EB%FF
2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В Основы криптографии. -Гелиос АРВ, 2002г., 402с.