**Лабораторная работа № 6. Исследование ассиметричных крипроалгоритмов**

**Цель работы: изучить и закрепить умение реализации криптосистемы RSA и криптосистемы Эль-Гамаля**

**Порядок выполнения работы:**

1. Изучить теоретический материал
2. Выбрать язык программирования
3. Выполнить практическую часть.
4. Оформить отчет. Отчет должен содержать:
   * наименование и цель работы;
   * ответы на контрольные вопросы;
   * код на выбранном языке программирования соответствующих заданий и скриншоты выполнения написанных программ;
   * выводы к выполненной лабораторной работе.

Отчет переименовать следующим образом: **ЗКИ\_ЛР6\_Фамилия\_№группы** и сдать на проверку преподавателю.

**Теоретическая часть**

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

RSA относится к так называемым *асимметричным алгоритмам*, у которых ключ шифрования не совпадает с ключом расшифровки. Один из ключей доступен всем и называется *открытым ключом*, другой хранится только у хозяина и никому неизвестен. С помощью одного ключа можно производить операции только в одну сторону. Если сообщение зашифровано с помощью одного ключа, то расшифровать его можно только с помощью другого. Имея один из ключей практически невозможно найти другой ключ, если разрядность ключа высока.

***Описание RSA***

Алгоритм RSA состоит из следующих пунктов:

1. Выбрать простые числа p и q.

2. Вычислить n = p\*q.

3. Вычислить m = (p – 1) \* (q – 1).

4. Выбрать число d взаимно простое с m.

5. Выбрать число e так, чтобы e\*d = 1 (mod m).

Числа e и d являются ключами RSA. Шифруемые данные необходимо разбить на блоки – числа от 0 до n – 1. Шифрование и расшифровка данных производятся следующим образом:

* шифрование: b = a e (mod n);
* расшифрование: a = bd (mod n).

Следует также отметить, что ключи e и d равноправны, то есть сообщение можно шифровать как ключом e, так и ключом d, при этом расшифровка должна быть произведена с помощью другого ключа.

Весь алгоритм расписан в таблице:

|  |  |  |
| --- | --- | --- |
| **Этап** | **Описание операции** | **Результат операции** |
| **Генерация ключей** | Выбрать два простых различных числа | p=3557,  q=2579 |
| Вычислить модуль (произведение) | n = p \cdot q = 3557 \cdot 2579 = 9173503 |
| Вычислить функцию Эйлера | \varphi(n) = (p-1) (q-1) = 9167368 |
| Выбрать открытую экспоненту | e = 3 |
| Вычислить секретную экспоненту | d = e^{-1} \mod \varphi(n)  d = 6111579 |
| Опубликовать открытый ключ | \{e, n\} = \{3,9173503 \} |
| Сохранить закрытый ключ | \{d, n\} = \{6111579, 9173503 \} |
| **Шифрование** | Выбрать текст для зашифровки | m = 111111 |
| Вычислить шифротекст | \begin{align} c &= E(m) \\  &= m^e \mod n \\  &= 111111^3   \mod 9173503 \\  &= 4051753 \end{align} |
| **Расшифрование** | Вычислить исходное сообщение | \begin{align} m &= D(c) = \\   &= c^d \mod n \\   &= 4051753^{6111579} \mod 9173503 \\   &= 111111 \end{align} |

# **Реализация элементов схемы шифрования Эль-Гамаля**

## **Генерация ключей**

1. Генерируется случайное простое число ~p длины ~n [битов](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82).
2. Выбирается случайный примитивный элемент ~g.
3. Выбирается случайное целое число ~x такое, что ~1 < x < p-1.
4. Вычисляется ~y = g^x\,\bmod\,p.
5. Открытым ключом является тройка \left( p,g,y \right), закрытым ключом - число ~x.

## **Шифрование**

Сообщение ~M шифруется следующим образом:

1. Выбирается сессионный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) — случайное целое число ~k такое, что ~1 < k < p - 1
2. Вычисляются числа a = g^k\,\bmod\,p и b = y^k M\,\bmod\,p.
3. Пара чисел \left( a, b \right) является [шифротекстом](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82).

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

## **Расшифрование**

Зная закрытый ключ ~x, исходное сообщение можно вычислить из шифротекста \left( a, b \right) по формуле:

M = b(a^x)^{-1}\,\bmod\,p.

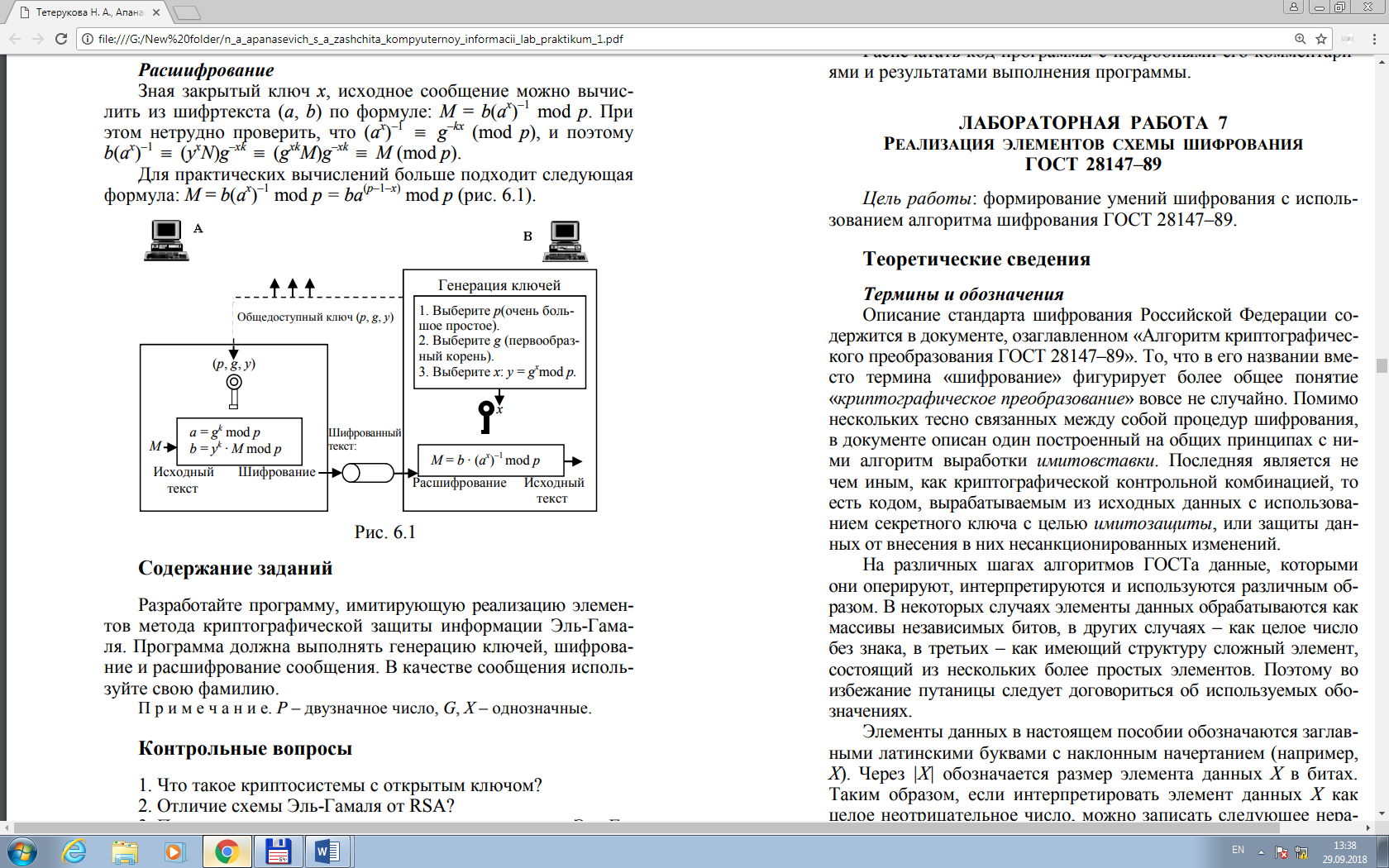
При этом нетрудно проверить, что

~(a^x)^{-1}\equiv g^{-kx}\pmod{p}

и поэтому

~b(a^x)^{-1}\equiv (y^kM)g^{-xk}\equiv (g^{xk}M) g^{-xk}\equiv M \pmod{p}.

Для практических вычислений больше подходит следующая формула:

M = b(a^x)^{-1}\,\bmod\,p = b \cdot a^{(p-1-x)}\,\bmod\,p  (рис. 6.1)

## **Пример**

**Шифрование**

Допустим что нужно зашифровать сообщение ~M=5.

Произведем генерацию ключей :

пусть ~p=11, g=2. Выберем ~x=8 - случайное целое число ~x такое,что ~1 < x < p.

Вычислим ~y= g^x\bmod{p}=2^8\bmod{11}=3.

Итак , открытым является тройка ~(p,g,y)=(11,2,3),а закрытым ключом является число ~x=8.

Выбираем случайное целое число ~k такое, что 1 < k < (p − 1). Пусть ~k=9.

Вычисляем число ~a=g^k\bmod{p}=2^9 \bmod{11}=512 \bmod{11}=6.

Вычисляем число ~b=y^k M\bmod{p}=3^9 5 \bmod{11}=19683 \cdot 5 \bmod{11}=9.

Полученная пара ~(a,b)=(6,9) является шифротекстом.

**Расшифрование**

Необходимо получить сообщение ~M=5 по известному шифротексту ~(a,b)=(6,9) и закрытому ключу ~x=8.

Вычисляем M по формуле : ~M=b(a^x)^{-1}\bmod{p}=9(6^8)^{-1}\mod{11}=5

Получили исходное сообщение ~M=5.

**Практическая часть**

**Задание №1**

Написать программу которая зашифрует и расшифрует текст введенный с клавиатуры, зашифрует и расшифрует его алгоритмом RSA.

Числа p и q выбрать самим.

В отчете должно сдержаться код программы, полученные результаты.

Код функции вычисления модуля на С++

template <typename T>

T modpow(T base, T exp, T modulus) {

base %= modulus;

T result = 1;

while (exp > 0) {

if (exp & 1) result = (result \* base) % modulus;

base = (base \* base) % modulus;

exp >>= 1;

} return result; }

**Задание №2**

Написать программу которая сгенерирует ключи, зашифрует и расшифрует текст введенный с клавиатуры алгоритмом Эль-Гамаля.

Ниже приведен пример программы реализующий данный алгоритм. Напишите на его примере программу обрабатывающую нашу задачу.

**Приложение: код рабочей программы на С++**

int power(int a, int b, int n){**// a^b mod n**

int tmp=a;

int sum=tmp;

for(int i=1;i<b;i++){

for(int j=1;j<a;j++){

sum+=tmp;

if(sum>=n){

sum-=n;

}

}

tmp=sum;

}

return tmp; }

int mul(int a, int b, int n){**// a\*b mod n**

int sum=0;

for(int i=0;i<b;i++){

sum+=a;

if(sum>=n){

sum-=n;

} }

return sum; }

**/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**p - простое число**

**0 < g < p-1**

**0 < x < p-1**

**m - шифруемое сообщение m < p**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/**

void crypt(int p,int g,int x, string inFileName,string outFileName){

ifstream inf(inFileName.c\_str());

ofstream outf(outFileName.c\_str());

int y=power(g,x,p);

wcout<<"Открытый ключ (p,g,y)="<<"("<<p<<","<<g<<","<<y<<")"<<endl;

wcout<<"Закрытый ключ x="<<x<<endl;

wcout<<"\nШифруемый текст:"<<endl;

while(inf.good()){

int m=inf.get();

if(m>0){   
 wcout<<(char)m;   
 int k=rand()%(p-2)+1; // 1 < k < (p-1)   
 int a= power(g,k,p);   
 int b= mul(power(y,k,p),m,p);   
 outf<<a<<" "<<b<<" "; } }   
 wcout<<endl;   
 inf.close();   
 outf.close(); }   
 void decrypt(int p,int x,string inFileName,string outFileName){   
 ifstream inf(inFileName.c\_str());   
 ofstream outf(outFileName.c\_str());   
 wcout<<"\nДешифрованый текст:"<<endl;   
 while(inf.good()){   
 int a=0;   
 int b=0;   
 inf>>a;   
 inf>>b;   
 if(a!=0&&b!=0){   
 //wcout<<a<<" "<<b<<endl;   
 int deM=mul(b,power(a,p-1-x,p),p);**// m=b\*(a^x)^(-1)mod p =b\*a^(p-1-x)mod p - трудно было найти нормальную формулу, в ней вся загвоздка**   
 char m=static\_cast<char>(deM);   
 outf<<m;   
 wcout<<m;   
 } }   
 wcout<<endl;   
 inf.close();   
 outf.close();   
}  
int main(){  
 srand(time(NULL));   
 crypt(593,123,8, "in.txt","out\_crypt.txt");   
 decrypt(593,8,"out\_crypt.txt","out\_decrypt.txt");  
 return 0; }

**Контрольные вопросы:**

* + 1. Дать определение понятию «Ассиметричный криптоалгоритм»
    2. Описать принцип крипросистемы RSA
    3. Описать принцип крипросистемы Эль-Гамаля
    4. Описать зашифровку текста алгоритмом Эль-Гамаля
    5. Описать расшифровку текста алгоритмом Эль-Гамаля