Белорусский государственный университет информатики и радиоэлектроники

Кафедра информатики

Лабораторная работа № 3

Асимметричная криптография. RSA.

Выполнила студент гр. 653502: Серебренников В. А.

Проверил ассистент КИ: Артемьев В. С.

Минск, 2019

Введение

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.

В рамках лабораторной работы необходимо реализовать программные средства шифрования и дешифрования при помощи алгоритма RSA.

Блок-схема алгоритма

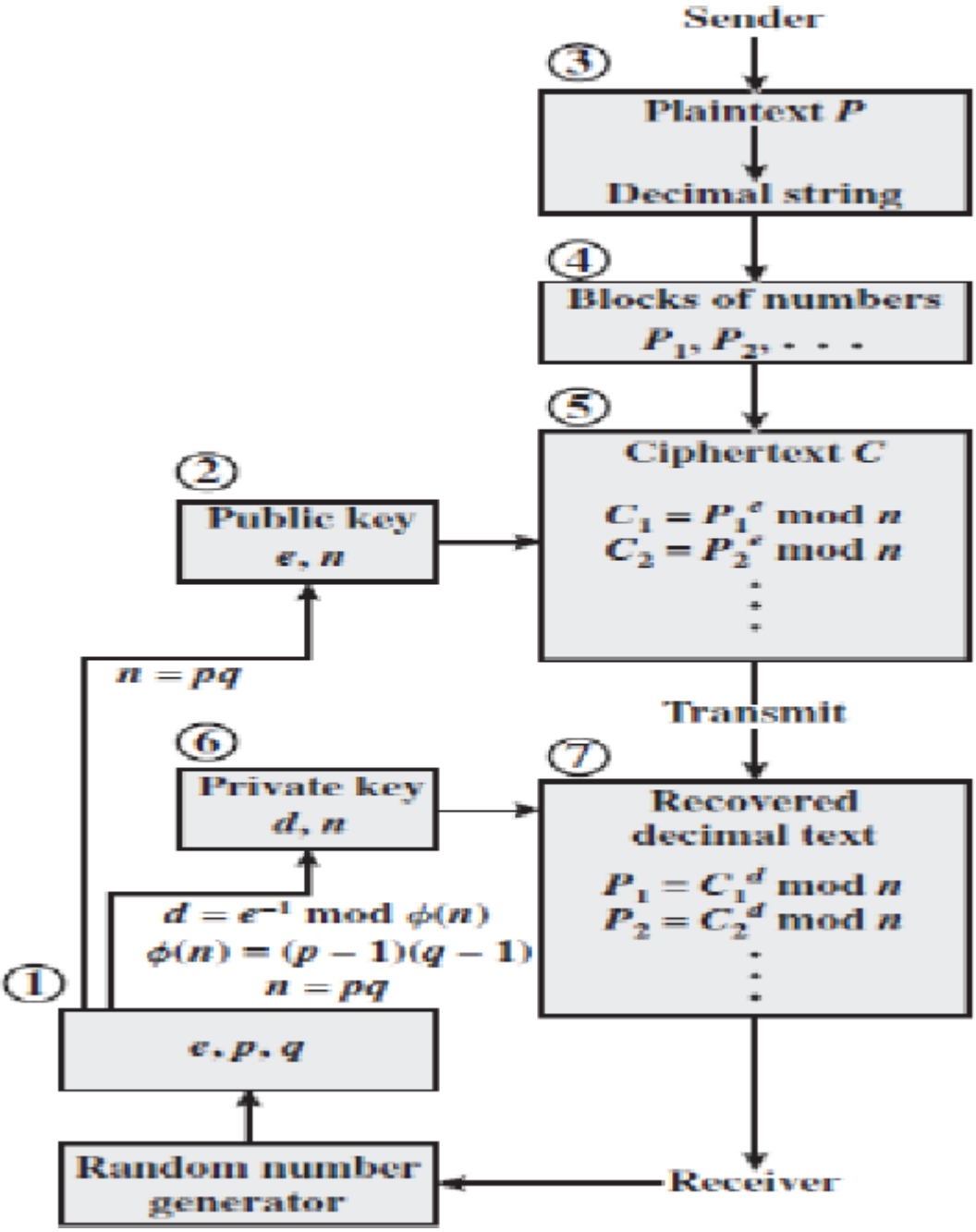

Рис.1. Схема алгоритма

Пример работы программы

```
p: 29 , q: 23
enc text :  [176, 317, 453, 137, 116, 9, 257, 271, 585, 538, 136, 52, 292,
 195, 9, 116, 137, 453, 317, 176]
dec text:  qwerty12345678ytrewq
```

Рис.2. Пример работы

Код программы

```
# -*- coding:utf-8 -*-

import math
import random

def gen_prime_num(max_num):
    prime_num=[]
    for i in range(2,max_num):
        temp=0
        sqrt_max_num=int(math.sqrt(i))+1
        for j in range(2,sqrt_max_num):
            if 0==i%j:
                temp=j
                break
        if temp==0:
            prime_num.append(i)

    return prime_num

def gen_rsa_key():
    prime=gen_prime_num(500)
    print(prime[-80:-1])
    while 1:
        prime_str=input("please choose two prime number from above: ").split(",")
        p,q=[int(x) for x in prime_str]
        if (p in prime) and (q in prime):
            break
        else:
            print("the number you enter is not prime number.")

    N=p*q
    r=(p-1)*(q-1)
    r_prime=gen_prime_num(r)
    r_len=len(r_prime)
    e=r_prime[int(random.uniform(0,r_len))]
    d=0
    for n in range(2,r):
        if (e*n)%r==1:
            d=n
            break

    return ((N,e),(N,d))

def encrypt(pub_key,origal):
    N,e=pub_key
    return (origal**e)%N

def decrypt(pri_key,encry):
    N,d=pri_key
    return (encry**d)%N

if __name__=='__main__':
    pub_key,pri_key=gen_rsa_key()
```

```
print("public key ",pub_key)
print("private key",pri_key)

origal_text=input("please input the origal text: ")
encrypt_text=[encrypt(pub_key,ord(x)) for x in origal_text]
decrypt_text=[chr(decrypt(pri_key,x)) for x in encrypt_text]

encrypt_show=",".join([str(x) for x in encrypt_text])
decrypt_show="".join(decrypt_text)
print("encrypt text: ",encrypt_show)
print("decrypt text: ",decrypt_show)
```

Вывод

В ходе написания лабораторной работы были изучены алгоритмы шифрования и дешифрования RSA, а также написаны их программные реализации. Были получены навыки усложнения и увеличения криптостойкости алгоритма RSA, а также изучены модификации и режимы работы алгоритма RSA.