|  |  |
| --- | --- |
| **Gerb-BMSTU_01** | **Министерство науки и высшего образования Российской Федерации**  Калужский филиал  федерального государственного бюджетного  образовательного учреждения высшего образования  ***«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»***  ***(КФ МГТУ им. Н.Э. Баумана)*** |

**ФАКУЛЬТЕТ** ***ИУК «Информатика и управление»***

**КАФЕДРА** \_\_***ИУК4 «Программное обеспечение ЭВМ, информационные технологии»***

**ЛАБОРАТОРНАЯ РАБОТА №3**

**«Алгоритм RSA. Обмен ключами симметричных алгоритмов с использованием ассиметричных криптосистем»**

**ДИСЦИПЛИНА: «Защита информации»**

|  |  |  |
| --- | --- | --- |
| Выполнил: студент гр. ИУК4-72Б | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ( Карельский М.К. )  (Подпись) |
| Проверил: | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ( Ерохин И.И. )  (Подпись) |
| Дата сдачи (защиты):  Результаты сдачи (защиты): | | |
|  | - Балльная оценка:  - Оценка: | |

Калуга, 2023

**Цель:** ознакомиться с математическими принципами функционирования алгоритма RSA. Научиться проводить шифрование/дешифрование с помощью данного алгоритма. Ознакомиться с принципом реализации обмена ключами с использованием схемы Диффи-Хеллмана.

**Задачи:** рассмотреть общие математические принципы организации процедуры шифрования/дешифрования при использовании метода RSA. Рассмотреть схему обмена ключами по алгоритму Диффи-Хеллмана. Реализовать программно алгоритм шифрования и дешифрования методом RSA. Провести шифрование открытого текста, выбранного согласно варианту, указанному преподавателем, и его последующее восстановление. Подготовить ответы на контрольные вопросы.

**Задание:**

1. Рассмотреть общие математические принципы организации процедуры шифрования/дешифрования при использовании метода RSA.
2. Рассмотреть схему обмена ключами по алгоритму Диффи-Хеллмана.
3. Реализовать программно алгоритм шифрования и дешифрования методом RSA.
4. Провести шифрование открытого текста, выбранного согласно варианту, указанному преподавателем, и его последующее восстановление.
5. Рассмотреть схему Диффи-Хеллмана с общим простым числом q и первообразным корнем a. Вами выбран секретный ключ Х\_А. При обмене ключами с вашим респондентом, имеющим открытый ключ Y\_B, вы получили от него общий секретный ключ К. Состоялся ли обмен ключами? Обоснуйте ответ. Вычислите значение открытого ключа Y\_A.

**Вариант 7**

* Открытый текст – интерполятор
* q = 71
* a = 7
* XA = 5
* YB = 11
* K = 23

**Листинг:**

import random, math

max\_prime = int(input('Введите максимально возможное значение p и q: '))

primes = [i for i in range(max\_prime + 1)]

primes[1] = 0

i = 2

while i <= max\_prime:

    if primes[i] != 0:

        j = i + i

        while j <= max\_prime:

            primes[j] = 0

            j = j + i

    i += 1

primes = [i for i in primes if i != 0]

primes.remove(2)

p = primes[random.randint(0, len(primes) - 1)]

primes.remove(p)

q = primes[random.randint(0, len(primes) - 1)]

if p\*q < 33:

    primes.remove(q)

    q = primes[random.randint(0, len(primes) - 1)]

print('p =', p)

print('q =', q)

n = p\*q

print('n =', n)

phi = (p - 1)\*(q - 1)

print('phi =', phi)

e = random.randint(2, phi - 1)

while math.gcd(e, phi) != 1:

    e = random.randint(2, phi - 1)

print('e =', e)

k = 1

while (k \* phi + 1) % e != 0:

    k += 1

d = (k \* phi + 1) // e

print('d =', d)

source = 'интерполятор'

encrypted = []

for s in source:

    s = ord(s) - 1072

    encrypted.append(s\*\*e % n)

print('Шифр:', encrypted)

decrypted = ''

for s in encrypted:

    decrypted += chr(s\*\*d % n + 1072)

print('Исходный текст:', decrypted)

print()

q = 71

a = 7

X\_A = 5

Y\_B = 11

K = 23

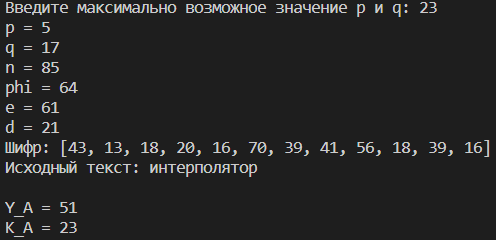
Y\_A = a\*\*X\_A % q

print('Y\_A =', Y\_A)

K\_A = Y\_B\*\*X\_A % q

print('K\_A =', K\_A)

**Результат:**



**Рис. 1.** Результат

Вычисленный ключ KA равен данному в условии ключу K, следовательно, обмен ключами состоялся.

**Вывод:** в ходе выполнения лабораторной работы были освоены математические принципы функционирования алгоритма RSA, принцип реализации обмена ключами с использованием схемы Диффи-Хеллмана, получены практические навыки шифрования/дешифрования с помощью RSA.