|  |  |
| --- | --- |
| **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 | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_Калашников А.С.\_\_)  (Подпись) (Ф.И.О.) |
| Проверил: | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_Ерохин И.И.\_\_\_)  (Подпись) (Ф.И.О.) |
| Дата сдачи (защиты):  Результаты сдачи (защиты): | | |
|  | - Балльная оценка:  - Оценка: | |

Калуга, 2023

**Целью выполнения** лабораторной работы является ознакомление с математическими принципами функционирования алгоритма RSA. Получение навыков шифрования/дешифрования с помощью данного алгоритма. Ознакомление с принципом реализации обмена ключами с использованием схемы Диффи-Хеллмана.

**Основными задачами** выполнения лабораторной работы являются:

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. Подготовить ответы на контрольные вопросы.

Результатами работы являются:

Разработанная программа согласно варианту задания

Подготовленный отчет

**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 . При обмене ключами с вашим респондентом, имеющим открытый ключ , вы получили от него общий секретный ключ К. Состоялся ли обмен ключами? Обоснуйте ответ. Вычислите значение открытого ключа .

**Листинг программы:**

import math

def fast\_pow(x, y):

if y == 0:

return 1

if y == -1:

return 1. / x

p = fast\_pow(x, y // 2)

p \*= p

if y % 2:

p \*= x

return p

def keygen(p, q):

n = p\*q

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

e = 0

i = 2

while i < euler:

e = math.gcd(euler, i)

if e == 1:

e = i

break

i += 1

d = 0

i = 2

while i < n:

if (i \* e) % euler == 1:

d = i

break

i += 1

keys = [e, d, n]

return keys

def encode(message, e, n):

return fast\_pow(message, e) % n

def decode(message, d, n):

return fast\_pow(message, d) % n

alphabet = ['а', 'б', 'в', 'г', 'д', 'е', 'ё', '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']

p = int(input("Введите простое число p: "))

q = int(input("Введите простое число q: "))

keys = keygen(p, q)

message = input("Введите сообщение для расшифровки: ")

symbols = list(message)

for i in range(0, len(symbols)):

for j in range(0, len(alphabet)):

if symbols[i] == alphabet[j]:

symbols[i] = j + 1

for i in range(0, len(symbols)):

symbols[i] = encode(symbols[i], keys[0], keys[2])

print(symbols)

for i in range(0, len(symbols)):

symbols[i] = decode(symbols[i], keys[1], keys[2])

for i in range(0, len(symbols)):

for j in range(0, len(alphabet)):

if symbols[i] == j + 1:

symbols[i] = alphabet[j]

print(symbols)

#Диффи-Хеллман

q = 17

a = 3

Xa = 6

Yb = 11

K = 12

print(math.pow(a, Xa) % q)

**Результат выполнения программы:**

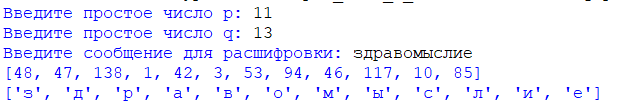




Рис.1. Результат работы

**Вывод:** в результате выполнения данной лабораторной работы были изучены математические принципы функционирования алгоритма RSA. Получениы навыки шифрования/дешифрования с помощью данного алгоритма. Ознакомление с принципом реализации обмена ключами с использованием схемы Диффи-Хеллмана.