Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Программирование криптографических алгоритмов

Обмен ключами по Диффи-Хеллману

Выполнила студентка 3 курса группы 171-341

Решетникова Дарья

Москва 2020 г.

Аннотация

Язык : Python

Программа: Visual Studio 2017

1. Описание шифра.

Протокол Диффи — Хеллмана (англ. Diffie-Hellman, DH) — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

2. Алгоритм шифра.

В протоколе обмена секретными ключами предполагается, что все пользователи знают некоторые числа **n** и **a** ($1 < a < n$). Для выработки общего секретного ключа пользователи A и B должны проделать следующую процедуру:

1. Определить секретные ключи пользователей K_A и K_B.

Для этого каждый пользователь независимо выбирает случайные числа из интервала (2,..., n-1).

2. Вычислить открытые ключи пользователей Y_A и Y_B.

Для этого каждый использует одностороннюю показательную функцию $Y=a^K \bmod n$ со своим секретным ключом.

3. Обменяться ключами Y_A и Y_B по открытому каналу связи.

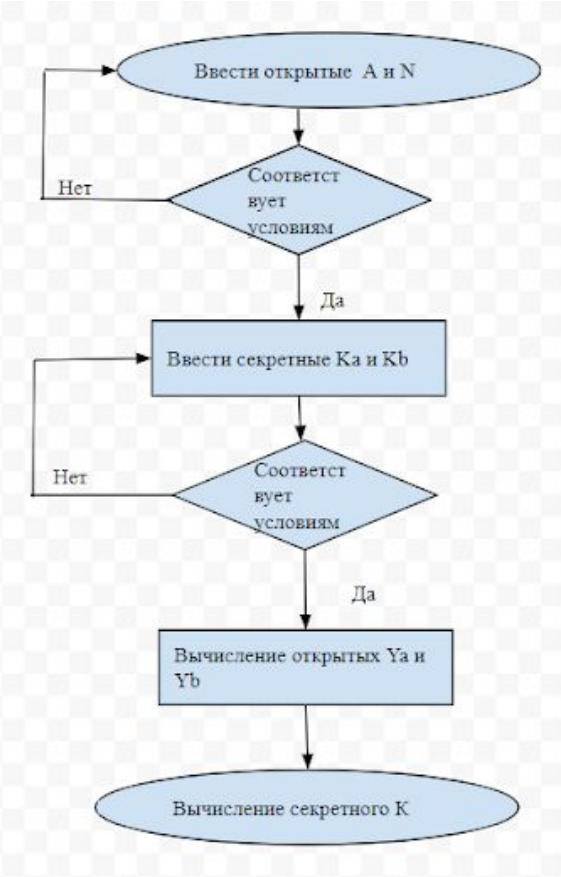
4. Независимо определить общий секретный ключ K.

Для этого пользователи выполняют вычисления с помощью той же односторонней функции

A: $Y_B^{KA} \pmod n = |a^{KB}|^{KA} \bmod n = a^{KA*KB} \bmod n = K.$

B: $Y_A^{KB} \pmod n = |a^{KA}|^{KB} \bmod n = a^{KB*KA} \bmod n = K.$

3. Блок-схема программы



4. Код программы

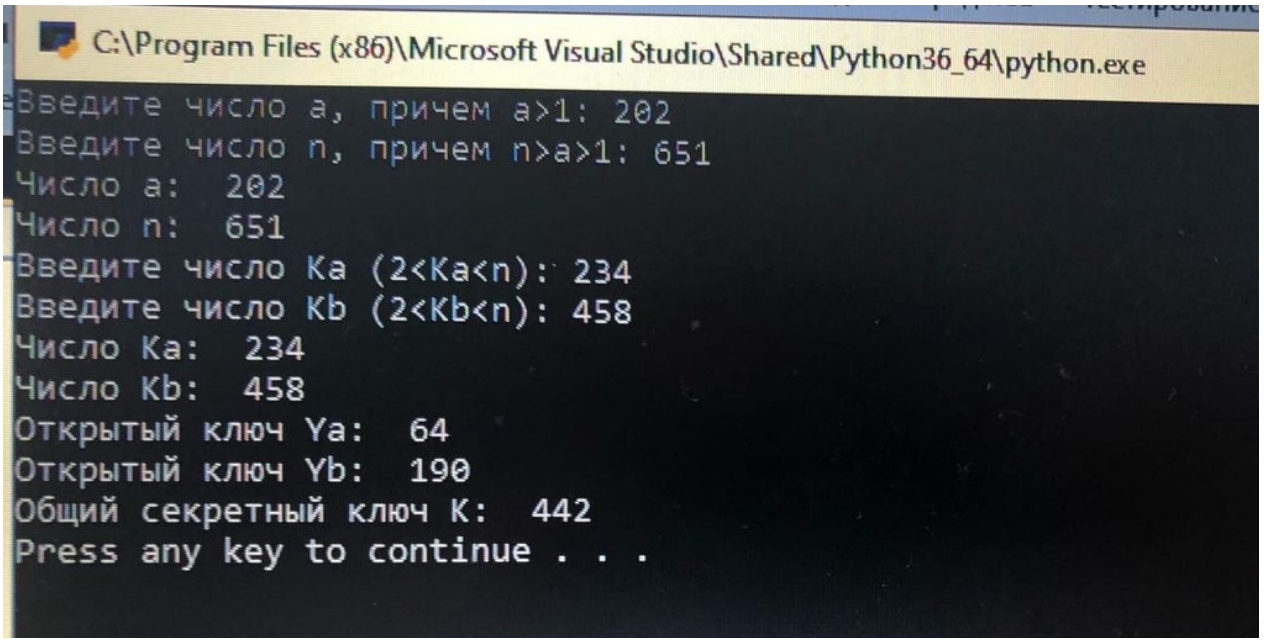
```
# некоторые числа a и n - открытые
a = int(input("Введите число a, причем a>1: "))
n = int(input("Введите число n, причем n>a>1: "))

while 1 >= a or a >= n:
    if a >= n or 1 >= n:
        n = int(input("Введенное число n не соответствует заданному условию. Введите повторно: "))
    elif 1 >= a:
        a = int(input("Введенное число a не соответствует заданному условию. Введите повторно: "))

print("Число a: ", a)
print("Число n: ", n)
# некоторые числа Ka и Kb - секретные ключи
Ka = int(input("Введите число Ka (2<Ka<n): "))
while 2 >= Ka or Ka >= n:
    Ka = int(input("Введенное число Ka не соответствует заданному условию. Введите повторно: "))

Kb = int(input("Введите число Kb (2<Kb<n): "))
while 2 >= Kb or Kb >= n :
    Kb = int(input("Введенное число Kb не соответствует заданному условию. Введите повторно: "))
while Ka == Kb:
    Kb = int(input("Числа Ka и Kb не должны быть равны. Введите Kb повторно: "))

print("Число Ka: ", Ka)
print("Число Kb: ", Kb)

# открытые ключи пользователей Ya и Yb
Ya = a ** Ka % n
print ("Открытый ключ Ya: ", Ya)
Yb = a ** Kb % n
print ("Открытый ключ Yb: ", Yb)
```

```
# обмен ключами Ya и Yb
# вычисляем K
K1 = Yb ** Ka % n
K11 = a ** (Kb*Ka) % n
```

```
K2 = Ya ** Kb % n
K22 = a ** (Ka*Kb) % n
```

```
if K1 == K2:
    print("Общий секретный ключ K: ", K2)
```

5. Тестирование



6. Исполняемый файл

Данная программа работает с окном выполнения программы, т.е. все действия совершаются там.