System Security

Monsoon Semester V 2021-22

Lab - 9

Date: 16th November 2021

Topic: Diffie-Hellman Key Exchange

AIM

Write a program to implement the Diffie-Hellman Key Exchange algorithm.

THEORY

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

- For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.

- P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

EXPERIMENT

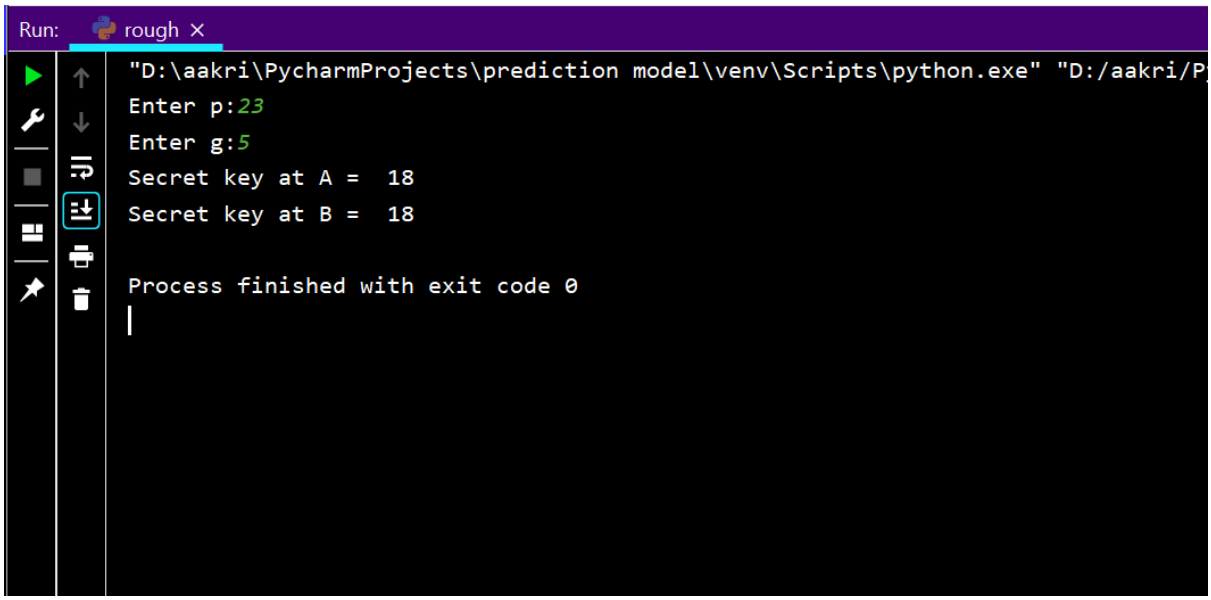
ALGORITHM:

1. Alice and Bob publicly agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 4$, then sends Bob $A = g^a \bmod p$
   - $A = 5^4 \bmod 23 = 4$
3. Bob chooses a secret integer $b = 3$, then sends Alice $B = g^b \bmod p$
   - $B = 5^3 \bmod 23 = 10$
4. Alice computes $s = B^a \bmod p$
   - $s = 10^4 \bmod 23 = 18$
5. Bob computes $s = A^b \bmod p$
   - $s = 4^3 \bmod 23 = 18$
6. Alice and Bob now share a secret (the number 18).

PROGRAM CODE

```
p = int(input("Enter p:"))
g = int(input("Enter g:"))
a = 4
b = 3
A = ((pow(g, a)) % p)
B = ((pow(g, b)) % p)
Ka = ((pow(B, a)) % p)
Kb = ((pow(A, b)) % p)
print("Secret key at A = ", str(Ka))
print("Secret key at B = ", str(Kb))
```

OUTPUT



CONCLUSION

Hence, Diffie-Hellman Key Exchange algorithm was implemented successfully.