

Experiment 6

Shashwat Shah

60004220126

TYBtech Comp B

Aim: Design and implement 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 elliptical 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, only prime P and G (a primitive root of P) and two private values a and b .

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

→ Alice and Bob get public numbers $P=23$ and $G=9$

→ Alice selected a private key — $a=4$

Bob selected a private key — $b=3$

→ Alice and Bob compute public values.

$$\begin{aligned}\text{Alice} - x &= (9^4 \bmod 23) = 6561 \bmod 23 = 6 \\ y &= (9^3 \bmod 23) = 729 \bmod 23 = 16\end{aligned}$$

→ Alice and Bob exchange public numbers.

→ Alice receives public key $y = 16$ and
Bob receives public key $x = 6$.

→ Alice and Bob compute symmetric keys

$$\text{Alice : } k_a = y^a \bmod p = 65536 \bmod 23 = 9$$

$$\text{Bob : } k_b = x^b \bmod p = 216 \bmod 23 = 9$$

→ 9 is the shared secret

Conclusion! Even while using ciphers for encryption, it is crucial that the key for encryption and decryption is secure and yet available to the sender and receiver. We learnt about the algorithm and implemented it in Python.



Academic Year: 2022-2023

EXPERIMENT 6

Shashwat Shah
TYBtech Comps B
C22
60004220126

AIM: Study and Implement Diffie Hellman Key Exchange Algorithm.

CODE:

```
from random import randint

P = 17
Q = 3

print('The Value of P is :%d'%(P))
print('The Value of Q is :%d'%(Q))

# Alice will choose the private key a
a = 4
print('The Private Key a for Alice is :%d'%(a))

# gets the generated key
x = int(pow(Q,a,P))

# Bob will choose the private key b
b = 3
print('The Private Key b for Bob is :%d'%(b))

# gets the generated key
y = int(pow(Q,b,P))

# Secret key for Alice
Alice_key = int(pow(y,a,P))

# Secret key for Bob
Bob_key = int(pow(x,b,P))

print('Secret key for the Alice is : %d'%(Alice_key))
print('Secret Key for the Bob is : %d'%(Bob_key))
```



Academic Year: 2022-2023

OUTPUT:

```
uments\BTech\Docs\6th Sem\IS\Code\Exp6\Diffie-Hellman.py"
The Value of P is :17
The Value of Q is :3
The Private Key a for Alice is :4
The Private Key b for Bob is :3
Secret key for the Alice is : 4
Secret Key for the Bob is : 4
PS C:\Users\Jadhav\Documents\BTech\Docs\6th Sem\IS\Code> █
```