NAME: PRERNA SUNIL JADHAV

SAP ID: 60004220127

BATCH: C2-2

BRANCH: COMPUTER ENGINEERING

COURSE: INFORMATION SECURITY LABORATORY.

COURSE CODE: DJ19CEL603

EXPERIMENT 06

AIM: Study and implement Diffie Hellman key Exchange Algorithm.

THEORY: Diffie Hellman key Exchange Algorithm was the first published public-key algorithm to appear in the seminal paper by Diffie-Hellman that defined public key cryptography and is generally refered to as Diffie-Hellman Algorithm.

The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.

The Algorithm itself is limited to the exchange of secret values.

The Algorithm depends for its effectiveness on the difficulty of computing discrete logarithm.

Algorithm:

Global Public Elements

q → Prime number

α → $\alpha < q$ & α is primitive root of q

User A Key Generation

Select private X_A → $X_A < q$

Calculate public Y_A → $Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B → $X_B < q$

Calculate public Y_B → $Y_B = \alpha^{X_B} \bmod q$

Calculation of secret key by A.

$K = (Y_B)^{X_A} \bmod q$

Calculation of secret key by B

$K = (Y_A)^{X_B} \bmod q$

Example:

If $p = 23$, $g = 5$, $A = 4$, $B = 3$. Solve using Diffie Hellman

→ $X_A = g^a \bmod p$ $\quad$ $X_B = g^b \bmod p$

$- 5^4 \bmod 23$ $\quad$ $= 5^3 \bmod 23$

$= 625 \bmod 23$ $\quad$ $= 125 \bmod 23$

$= 4$ $\quad$ $= 10$

$A_K = (X_B)^a \bmod p = 10^4 \bmod 23$ $\quad$ $\boxed{\therefore A_K = 18}$

$B_K = (X_A)^b \bmod p = 4^3 \bmod 23$ $\quad$ $\boxed{\therefore B_K = 18}$

$\boxed{\therefore A_K = B_K = 18}$ → Now ~~they~~ 2 parties can communicate

CONCLUSION: The security of the algo lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible.

Shri Vile Parle Kelavani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)

Academic Year: 2022-2023

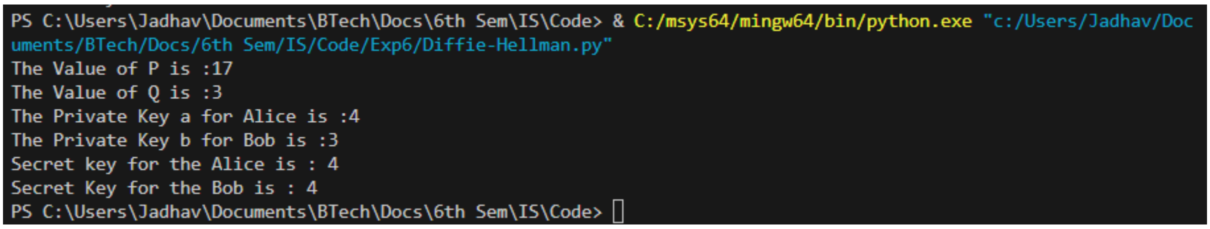
Name:	Prerna Sunil Jadhav
Sap Id:	60004220127
Class:	T. Y. B. Tech (Computer Engineering)
Course:	Information Security Laboratory
Course Code:	DJ19CEL603
Experiment No.:	06

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))
```

OUTPUT:



```
PS C:\Users\Jadhav\Documents\BTech\Docs\6th Sem\IS\Code> & C:/msys64/mingw64/bin/python.exe "c:/Users/Jadhav/Doc
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> 
```