**Experiment No. 6**

**Title:** Diffie-Hellman Key Exchange Protocol

**Batch: Roll No.: Experiment No.:**

**Title:** Perform VLab andimplement Diffie-Hellman key exchange protocol.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Resources needed:** Windows/Linux OS

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Theory:**

To implement Diffie-Hellman, the two end users Alice and Bob, while communicating over a

channel they know to be private, mutually agree on positive whole numbers p and q, such

that p is a prime number and q is a generator of p. The generator q is a number that, when

raised to positive whole-number powers less than p, never produces the same result for any

two such whole numbers. The value of p may be large but the value of q is usually small.

Once Alice and Bob have agreed on p and q in private, they choose positive whole-number

personal keys a and b, both less than the prime-number modulus p. Neither user divulges

their personal key to anyone; ideally they memorize these numbers and do not write them

down or store them anywhere. Next, Alice and Bob compute public keys a\* and b\* based on

their personal keys according to the formulas

a\* = qa mod p

and

b\* = qb mod p

The two users can share their public keys a\* and b\* over a communications medium assumed

to be insecure, such as the Internet or a corporate wide area network (WAN). From these

public keys, a number x can be generated by either user on the basis of their own personal

keys. Alice computes x using the formula

x = (b\*)a mod p

Bob computes x using the formula

x = (a\*)b mod p

The value of x turns out to be the same according to either of the above two formulas.

However, the personal keys a and b, which are critical in the calculation of x, have not been

transmitted over a public medium. Because it is a large and apparently random number, a

potential hacker has almost no chance of correctly guessing x, even with the help of a

powerful computer to conduct millions of trials. The two users can therefore, in theory,

communicate privately over a public medium with an encryption method of their choice using the decryption key x.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Algorithm :**

1. Perform Vlab - https://cse29-iiith.vlabs.ac.in/exp/diffie-hellman/index.html
2. Make use of client-server chatting applicationand implement following
3. **Client/Sender**
4. Choose a large prime number *p*
5. Calculate generator *g* of *p*
6. Share *p* and *g* with the Server/Receiver
7. Select any natural number (client secrete) *a*
8. *Calculate RA = ga mod p* and send it to the Server/Receiver
9. Upon receiving RB from the Server/Receiver, calculate shared key KAB = (RB )a *mod* *p*
10. **Server/Receiver:**
11. Select any natural number (server secrete) *b*
12. Upon receiving *p* and *g*, calculate *RB = ba mod p* and send it to the Client/Sender
13. Upon receiving RA from the Client/Sender, calculate shared key KAB = (RA )b *mod* *p*
14. **NOTE/OBSERVE :** Manually verify that theKAB at both the ends is same.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Questions:**

1. Explain any one attack on Diffie-Hellman key exchange protocol.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Outcomes:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion:**

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**References:**

**Books/ Journals/ Websites:**

* Mark Stamp, “Information security Principles and Practice” Wiley.