Sudesh Pawar
F17111037 (24)
BE Comp A

ICS A5

Q.1) Explain Diffie-Hellman Key-exchange algorithm?

Ans. The Diffie-Hellman algorithm provides a way of generating a shared secret between the sender & the receiver insuch a way that the secret need not be exchanged or transferred over the communication medium.

i) Alex chooses 2 prime nos. g & p and also a secrent number a. He calculates value of A such that $A = g^a \bmod p$. He then sends y, p and A to Bobby.

ii) Similarly, Bobby chooses a secret no. b & computes the value of B such that $B = g^b \bmod p$.

iii) Alex computes shared key at his end as shared key, $S = A \bmod p$.

iv) Bobby ~~completes~~ computes shared key S, derived in Step 3 & 4 are equal due to mod operation.

$$(g^a \bmod p)^b \bmod p = g^b \bmod p$$

$$(y^b \bmod p)^a \bmod p = g^a \bmod p$$

Q.2) Define:

1) PublicKey : Public Key is the key which is publicly known to the people & organization.

2) PrivateKey : Private Key is the key which is only known to the organization itself and kept as secret outside the organization.

Q.3) Suppose that 2 parties A & B agree on 7 as modulus, 3 as the primitive root. A chooses 2 & B chooses 5 as their respective secrets. Find Diffie Hellman Key.

Ans. $a = 2, b = 5, g = 3, p = 7$

$A = g^a \bmod p$

$A = 3^2 \bmod 7$

$= 9 \bmod 7$

$= 2$

$B = g^b \bmod p$

$B = 3^5 \bmod p.$

$= 243 \bmod 7$

$= 5$

A and B exchange A' and B'

A calculates S as

$S = B^a \bmod p.$

$= 5^2 \bmod 7.$

$= 25 \bmod 7 = 4$

B calculates S as,

$S = A^b \bmod p$

$= 2^5 \bmod 7 = 32 \bmod 7 = 4.$

So the shared key between organization A & B is 4.