Asynchronous Session Activity

Diffie Hellman Key Exchange Algorithm

→ The Diffie-Hellman [DH] Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the internet.
DH enables the two to use a public key to encrypt and decrypt their conversation o data using symmetric cryptography.

The Algorithm

Consider User A & B, who wants to exchange their message.
User A will have his own private key (say K) and
User B will have his own privat key (say L)
So, first they will make a cipher text —

$$A = p^K \bmod q$$

where A - Cipher text
q & p^K - prime no.
K - A's private key

$$B = p^L \bmod q$$

where L is B' private key

Now they will exchange their cipher texts then they will find the private keys of each other. through messaging (Secret key)

Now to find the private key,

for User A

$S = B^k \bmod q$

for User B

$S = A^L \bmod q$

Now the result will be same, that is, they have successfully exchanged and decrypted the messages (Secret Encryption key)

Numerical Example

Lets take two prime no.

G: 233 N: 601

User A's X value – 21

User B's Y value – 9

User A's A value – 185

$A = G^x \bmod N$

User B's B value – 588

$B = G^y \bmod N$

Now, User A will send his A value to User B and User B will send his B value to User A, then they will recalculate the values to set the same shared key.

User A key – 588

$key = B^x \bmod N$

User B key – 588

$Key = A^y \bmod N$

The key matched.

Hence they shared information successfully.

— by Udit Gupta
204762
2 MCA