Name - Tibi Saju
Rollno: 2047261
2 MCA

CN Asynchronous Activity

Diffie Hellman Key Exchange Algorithm

Diffie Hellman is a standard method of UserA & User B being able to communicate and end up with the same secret encryption key. This will make the attacker very difficult to retreive the secret key.

Algorithm

Consider User A and UserB, who wants to exchange their message.

User A will have his private key (Say a) and User B will have his private key (say b)

So first they will make a cipher text

$A = p^a \bmod q$

$B = p^b \bmod q$

Where p = primitive root
q = prime number
a = A's private key

where b = B's private Key.

Now they will exchange there cipher texts

Then they will find the private keys of each others message (Secret key)

Now to find ther private key,

For User A

$S = B^a \bmod q$

User B

$S = A^b \bmod q$

Now the result(s) will be same, that is, that have successfully exchanged and decrypted the messages (secret encryption key)

Numerical Example

Consider $q = 13$, $p = 6$ (q = prime number, p = primitive root)

User A

Private key $a = 3$

$A = 6^3 \bmod 13$

$A = 8$

User B

Private key $b = 10$

$B = 6^{10} \bmod 13$

$B = 4$

Now they exchange their public values A & B.

Now after Exchange

User A	User B
B = 4	A = 8
Now for retrieving the actual value,	
$S = B^a \bmod 13$	$S = A^b \bmod 13$
Where a = A's private key	Where b = b's private key
B = User B's public value (key)	A = User A's public value. (key)
$S = 4^3 \bmod 13$	$S = 8^{10} \bmod 13$
S = 12	S = 12

Hence they received the result (secret encryption key) successfully.