**Diffie Hellman Key Exchange**

Since the network is not secured if the secret key is passed with out encryption then a person in the middle can see the message being transferred and can change the message in his own language.

Example:-

|  |  |  |
| --- | --- | --- |
| **User A** | **Man in the Middle** | **User B** |
|  |  |  |
| **User A** generates a secret key(**SA** = 5)­ with which he will be encrypting his message. |  | **User B** generates a secret key(**SB** = 9) with which he will be encrypting his message. |
| **User A** sends **SA**to **User B** since **User B** needs to decrypt the message sent by **User A**. | While transferring he gets to know **SA** = 5 and changes **SA**= 8. | **User B** gets **SA** = 8. |
| **User B** gets **SA** = 3. | While transferring he gets to know **SB** = 9 and changes **SB**= 3. | **User B** sends **SB**to **User A** since **User A** needs to decrypt the message sent by **User B**. |
| **User A** sends a message encrypted using **SA** = 5. | He gets the message and since he knows the original **SA** = 5 he decrypts the message and he comes to know everything that **User A** was transferring to **User B**. | **User B** tries to decrypt the message sent by **User A** using **SA** = 8. Since this was changed by the **Man in the Middle**. But he fails to do so. |
| **User A** tries to decrypt the message sent by **User B** using **SB** = 3. Since this was changed by the **Man in the Middle**. But he fails to do so. | He gets the message and since he knows the original **SB** = 9 he decrypts the message and he comes to know everything that **User B** was transferring to **User A**. | **User B** sends a message encrypted using **SB** = 9. |
| He has the wrong message. | He knows messages sent by both the users. | He has the wrong message. |

So, the message transfer in this method was not secure.

To secure the message transfer an encryption key needs to be generated but it cannot be passed over the network. This key needs to calculated by the user so that it is not intercepted as it is not transferred over a unsecured network.

Algorithm:-

Step 1 :- **User A** and **User B** agree to use a **prime number p** = 13 and a **generator g = 4**. These are the public keys.

Step 2 :- **User A** chooses a **secret(private key) integer a** = 3

Sends to **User B**, **A = ga mod p**

**A = 43 mod 13**

**A = 64 mod 13**

Sends **A = 12**

Step 3 :- **User B** chooses a **secret(private key) integer b** = 6

Sends to **User A**, **B = gb mod p**

**B = 46 mod 13**

**B = 4,096 mod 13**

Sends **B = 1**

Step 4 :- **User A** computes **SA = Ba mod p**

**SA = 13 mod 13**

**SA = 1 mod 13**

**SA = 1**

Step 5 :- **User B** computes **SB = Ab mod p**

**SB = 126 mod 13**

**SB = 2,985,984 mod 13**

**SB = 1**

Step 6 :- **User A** and **User B** now share a secret: **SA = SB = 1**. This is because **3\*6** is the same as **6\*3**. So somebody who comes to know both these private integers might calculate S as follows:

**S = 43\*6 mod 13**

**S = 46\*3 mod 13**

**S = 418 mod 13**

**S = 68,719,476,736 mod 13**

**S = 1**

So the Man in the Middle can stop the attack since the Secret Private Keys are not transferred over the network.

Keys known to and transferred by **User A** and **User B** :-

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **User A** | | | **Man in the Middle** | **User B** | | |
| **Private** | **Public** | **Calculates** | **Sends** | **Calculates** | **Public** | **Private** |
| a | p, g |  | p, g |  |  | b |
| a | p, g, A | ga mod p = A | A |  | p, g | b |
| a | p, g, A |  | B | gb mod p = B | p, g, A, B | b |
| a, SA | p, g, A, B | Ba mod p = SA |  | Ab mod p = SB | p, g, A, B | b, SB |

To show who knows what :-

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **User A** | | **User B** | | **Man in the Middle** | |
| **knows** | **doesn’t know** | **knows** | **doesn’t know** | **knows** | **doesn’t know** |
| p = 13 | **b = ?** | p = 13 | **a = ?** | p = 13 | **a = ?** |
| g = 4 |  | g = 4 |  | g = 4 | **b = ?** |
| a = 3 |  | b = 6 |  |  | **S = ?** |
| A = 43 mod 13 = 12 |  | B = 46 mod 13 = 1 |  | A = 4a mod 13 = 12 |  |
| B = 4b mod 13 = 1 |  | A = 4a mod 13 = 12 |  | B = 4b mod 13 = 1 |  |
| SA = 13 mod 13 = 1 |  | SB = 126 mod 13 = 1 |  | SA = 1a mod 13 |  |
| SB = 12b mod 13 = 1 |  | SA = 1a mod 13 = 1 |  | SB = 12b mod 13 |  |
| SA = 13 mod 13 = 12b mod 13 = SB |  | SB = 126 mod 13 = 1a mod 13 = SA |  | SA = 13 mod 13 = 12b mod 13 = SB  **OR**  SB = 126 mod 13 = 1a mod 13 = SA |  |
| SA = 1 |  | SB = 1 |  |  |  |

So here we can see that the Man in the Middle does not know the encryption key SA = SB  = S which is calculated by User A and User B. So the users can send messages encrypted using the secret key and no attacks are made on the message.