1 Solution

In the Diffie-Hellman Key Exchange Protcol, the following steps are taken to securely transfer message over a public channel:

1. Alice and Bob agree on a prime number p and a base g such that $1 < g < p$ and an encryption algorithm they will later use

2. Alice chooses a secret integer a and sends Bob $A \equiv g^a \mod p$.

3. Bob chooses a secret integer b and sends Alice $B \equiv g^b \mod p$.

4. Alice use her own number a and number B from Bob to compute the shared secret key $k = B^a \equiv (g^b)^a \mod p$

5. Bob use his own number b and number A from Alice to compute the shared secret key $k = A^b \equiv (g^a)^b \mod p$

6. Then Alice sends Bob the message encrypted with the shared secret key k using a known encryption algorithm.

7. Bob decrypts the message with the shared secret key k.

2 Example

Now let's use actual numbers to demonstrate the Diffie-Hellman Key Exchange Protocol.

1. Let $p = 29$ and $g = 5$.

2. Alice chooses a secret integer $a = 4$ and sends Bob $g^a \mod p = 5^4 \mod 29 = 625 \mod 29 = 16$.

3. Bob chooses a secret integer $b = 3$ and sends Alice $g^b \mod p = 5^3 \mod 29 = 125 \mod 29 = 9$.

4. Alice uses her own number $a = 16$ and number $B = 9$ from Bob to compute the shared secret, $k = 9^4 \mod 29 = 7$.

4. Bob uses his own number $a = 3$ and number $A = 16$ from Alice to compute the shared secret, $k = 16^3 \mod 29 = 7$.

5. Now Alice sends Bob the message encrypted with the shared secretkey $k = 7$ using a known encryption algorithm.

6. Bob decrypts the message with the shared secret key $k = 7$.