Diffie Hellman Key Exchange Algorithm

The Diffie Hellman Key Exchange Algorithm was developed by Whitfield Diffie and Martin Hellman. It is used to generate symmetric cyptographic key at sender as well as receiver end so that there is no need to transfer key from sender to receiver.

If sender and receiver want to communicate with each other they first need to agree on the same key generated by Diffie Hellman algorithm, later on they can use this key for encryption or decryption.

Algorithm

1. Alice & Bob agree upon modulus p & base g.

Algorithm

1. Alice & Bob agree upon modulus p & base g.

2. Sender (Alice) selects another secret large random number $\underline{a}$ and calculates X_A

$$\Rightarrow \quad X_A = g^a \bmod p$$

. Alice then sends X_A to Bob (Receiver)

Algorithm

1. Alice & Bob agree upon modulus p & base g.

2. Sender (Alice) selects another secret large random number $\underline{a}$ and calculates X_A

$$\Rightarrow \quad X_A = g^a \bmod p$$

. Alice then sends X_A to Bob (Receiver)

3. Bob selects another secret large random number $\underline{b}$ & calculates X_B

$X_B \Rightarrow g^b \bmod p$. Bob sends X_B to Alice.

Algorithm

1. Alice & Bob agree upon modulus p & base g.

2. Sender (Alice) selects another secret large random number $\underline{a}$ and calculates X_A

$\Rightarrow \quad X_A = g^a \bmod p$. Alice then sends X_A to Bob (Receiver)

3. Bob selects another secret large random number $\underline{b}$ & calculates X_B

$X_B \Rightarrow g^b \bmod p$. Bob sends X_B to Alice.

4. Alice calculates the secret key $A_K = (X_B)^a \bmod p$

Algorithm

1. Alice & Bob agree upon modulus p & base g.

2. Sender (Alice) selects another secret large random number a and calculates X_A

   $\Rightarrow X_A = g^a \bmod p$. Alice then sends X_A to Bob (Receiver)

3. Bob selects another secret large random number b & calculates X_B

   $X_B \Rightarrow g^b \bmod p$. Bob sends X_B to Alice.

4. Alice calculates the secret key $A_K = (X_B)^a \bmod p$

5. Bob calculates the secret key $B_K = (X_A)^b \bmod p$

Algorithm

If $A_k = B_k$, then Alice & Bob can agree for future communication.

Solved Examples

1. If $p = 23$, $g = 5$, $A = 4$, $B = 3$. Solve Using Diffie Hellman Algorithm

Solved Examples

1. If $p = 23$, $g = 5$, $A = 4$, $B = 3$. Solve Using Diffie Hellman Algorithm

<u>Sol:</u>

$$X_A = g^a \bmod p$$

$$= (5)^4 \bmod 23$$

$$= (625) \bmod 23$$

$$= 4$$

Solved Examples

1. If $p = 23$, $g = 5$, $A = 4$, $B = 3$. Solve Using Diffie Hellman Algorithm

Sol:

$$X_A = g^a \bmod p$$

$$= (5)^4 \bmod 23$$

$$= (625) \bmod 23$$

$$= 4$$

$$X_B = g^b \bmod p$$

$$= (5)^3 \bmod 23$$

$$= (125) \bmod 23$$

$$= 10$$

Solved Examples

1. If $p = 23$, $g = 5$, $A = 4$, $B = 3$. Solve Using Diffie Hellman Algorithm

<u>Sol:</u> Alice calculates her secret key A_k as :

$$A_k = (X_B)^a \bmod p$$

$$= (10)^4 \bmod 23$$

$$\boxed{A_k = 18}$$

Solved Examples

1. If $p = 23$, $g = 5$, $A = 4$, $B = 3$. Solve Using Diffie Hellman Algorithm

Sol: Bob calculates his secret key B_K as :

$$B_K = (X_A)^b \bmod p$$

$$= (4)^3 \bmod 23$$

$$= 256 \bmod 23$$

$$\boxed{B_K = 18}$$

Solved Examples

1. If $p = 23$, $g = 5$, $A = 4$, $B = 3$. Solve Using Diffie Hellman Algorithm

As $A_K = B_K = 18$.

They can now start communicating with each other using this shared secret key.

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

$$= g^{ab} \bmod p$$

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

$$= g^{ab} \bmod p$$

$$= g^{ba} \bmod p$$

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

$$= (X_B)^a \bmod p$$

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

Only a & b are kept secret, All the other values :

p, g, $g^a \bmod p$ & $g^b \bmod p$ are sent in cleartext.

Only a & b are kept secret, All the other values :

$p, g, g^a \bmod p$ & $g^b \bmod p$ are sent in cleartext.

The strength of the scheme comes from the fact that

$$g^{ab} \bmod p = g^{ba} \bmod p$$

takes extremely long time to compute by any known algorithm just from the knowledge of $p, g, g^a \bmod p$ & $g^b \bmod p$.

This is called as the Discrete Log Problem.

For example,

If I know g, $g^a \bmod p$ & $g^b \bmod p$ & even p.

Can I solve $g^{ab} \bmod p$ or $g^{ba} \bmod p$??

The answer is NO or extremely difficult.

i.e If you have g^a or g^b, what is g^{ab}?

As $g^a \cdot g^b = g^{a+b}$, Also

$g^a \cdot g^b \neq g^{ab}$

for ex.

$2^5 = 2^{4+1} = 2^4 \cdot 2^1$

but $2^5 \neq 2^{4 \cdot 1}$ where

$a=4, b=1$

Example 2

$p = 7, \quad g = 17, \quad a = 6, \quad b = 4$

Example 3

$p = 353, \quad g = 3, \quad a = 97, \quad b = 233$

Example 4

$p = 11, \quad g = 2, \quad a = 9, \quad b = 3$

(If A has public key 9, find A's private key)

(If B has public key 3, find B's private key)