

# 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 cryptographic 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.**



Sender

Receiver

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  $a$  and calculates

$X_A$   
 $\Rightarrow X_A = g^a \pmod p$  . 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  $a$  and calculates

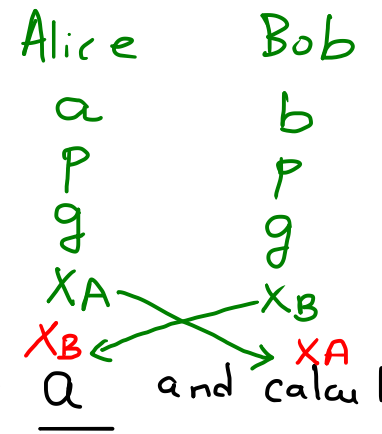
$X_A$

$\Rightarrow \underline{X_A = g^a \text{ mod } p}$  . Alice then sends  $X_A$  to Bob (Receiver)

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

$X_B \Rightarrow g^b \text{ mod } p$  . 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  $a$  and calculates

$X_A$

$\Rightarrow X_A = g^a \text{ mod } p$  . Alice then sends  $X_A$  to Bob (Receiver)

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

$X_B \Rightarrow g^b \text{ mod } p$  . Bob sends  $X_B$  to Alice.

4. Alice calculates the secret key  $A_K$  =  $(X_B)^a \text{ mod } p$

# Algorithm

1. Alice & Bob agree upon modulus p & base g.
  2. Sender (Alice) selects another secret large random number  $a$  and calculates  $X_A$   
 $\Rightarrow X_A = g^a \pmod p$ . Alice then sends  $X_A$  to Bob (Receiver)
  3. Bob selects another secret large random number  $b$  & calculates  $X_B$   
 $X_B \Rightarrow g^b \pmod p$ . Bob sends  $X_B$  to Alice.
  4. Alice calculates the secret key  $A_K = (X_B)^a \pmod p$
  5. Bob calculates the secret key  $B_K = (X_A)^b \pmod p$
- $A_K = B_K$   
 $S_K$
-

# 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

Sol:  $X_A = g^a \text{ mod } p$

  $= (5)^4 \text{ mod } 23$

$$= (625) \text{ mod } 23$$

$$= 4$$

## Solved Examples

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

Sol:

$$\begin{aligned} X_A &= g^a \pmod p \\ &= (5)^4 \pmod{23} \\ &= (625) \pmod{23} \\ &= 4 \end{aligned}$$

$$\begin{aligned} X_B &= g^b \pmod p \\ &= (5)^3 \pmod{23} \\ &= (125) \pmod{23} \\ &= 10 \end{aligned}$$

## Solved Examples

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

Sol: Alice calculates her secret key  $A_k$  as:

$$\begin{aligned} A_k &= (X_B)^a \text{ mod } p \\ &= (10)^4 \text{ mod } 23 \end{aligned}$$

$$A_k = 18$$

## 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 :

$$\begin{aligned} B_K &= (X_A)^b \text{ mod } p \\ &= (4)^3 \text{ mod } 23 \\ &= 256 \text{ mod } 23 \end{aligned}$$

$$\boxed{B_K = 18}$$

## 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.

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

$B_k$

$(g^a \bmod p)$

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

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

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

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

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

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

$X_B$

$$2^3^2 \Rightarrow 2^3$$

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

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  $p, g, g^a \bmod p$  &  $g^b \bmod p$ .

$a, b \rightarrow$  Unknown

This is called as the **Discrete Log Problem**.

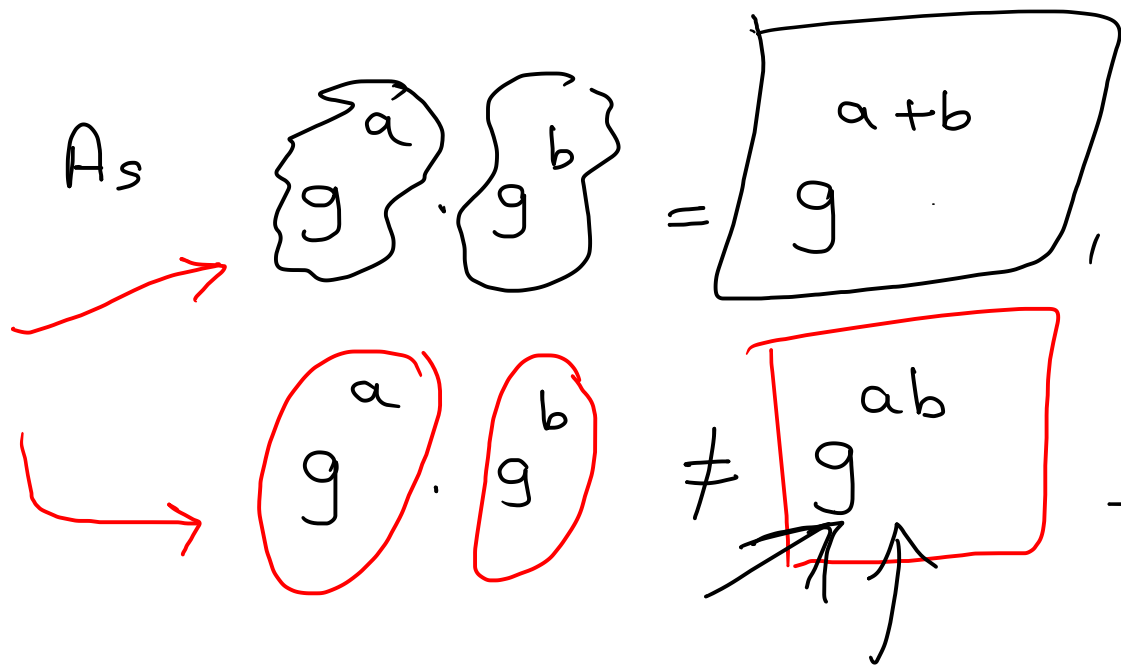
For example,

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

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

The answer is NO or extremely difficult.

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



Also

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

for ex.

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

but

$$2^5 \neq \boxed{2^{4 \cdot 1}}$$

where  
 $a=4, b=1$

2

## 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)

## Example 2

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

Sol:      Step 1:      Calculate  $X_A$ , (Public Component of A)

$$X_A = g^a \text{ mod } p$$

## Example 2

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

Sol: Step 1: Calculate  $X_A$ , (Public Component of A)

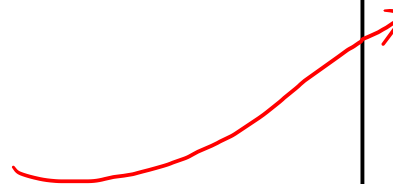
$$\begin{aligned} X_A &= g^a \text{ mod } p \\ &= 17^6 \text{ mod } 7 \end{aligned}$$

## Example 2

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

Sol: Step 1: Calculate  $X_A$ , (Public Component of A)

$$\begin{aligned} X_A &= g^a \pmod p \\ &= (17)^6 \pmod 7 \end{aligned}$$


$$\begin{aligned} 17^1 \pmod 7 &= 3 \\ 17^2 \pmod 7 &= 2 \quad \checkmark \\ 17^4 \pmod 7 &= 4 \quad \checkmark \\ \therefore 17^6 \pmod 7 &= 17^{2+4} \pmod 7 \\ &= 8 \pmod 7 \end{aligned}$$

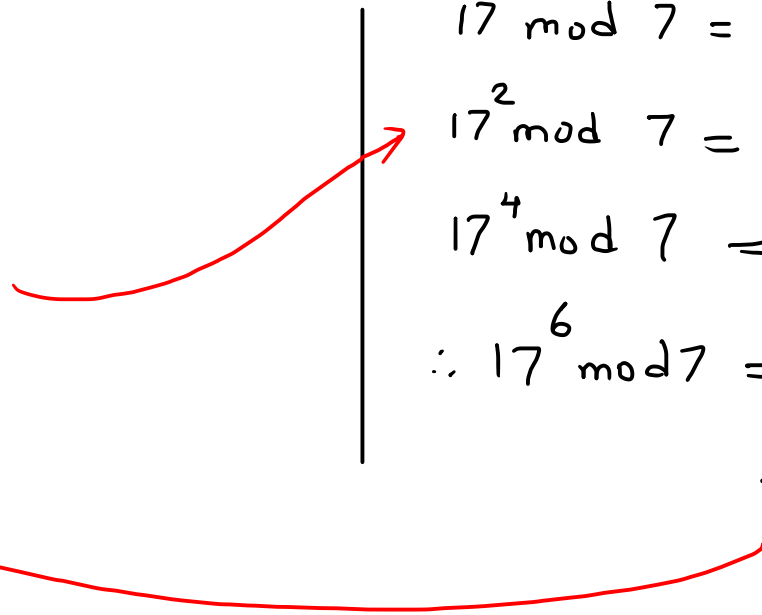
Example 2

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

Sol: Step 1: Calculate  $X_A$ , (Public Component of A)

$$\begin{aligned} X_A &= g^a \text{ mod } p \\ &= (17)^6 \text{ mod } 7 \\ &= 1 \end{aligned}$$

$$\begin{aligned} 17^1 \text{ mod } 7 &= 3 \\ 17^2 \text{ mod } 7 &= 2 \checkmark \\ 17^4 \text{ mod } 7 &= 4 \checkmark \\ \therefore 17^6 \text{ mod } 7 &= 17^{2+4} \text{ mod } 7 \\ &= 8 \text{ mod } 7 \end{aligned}$$



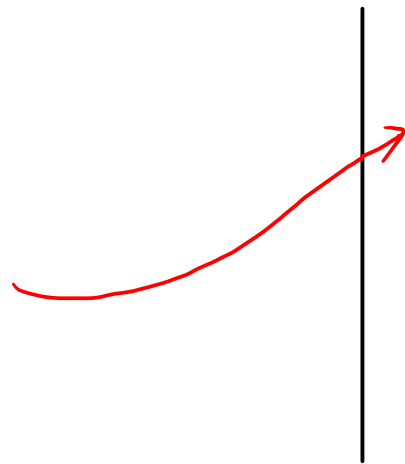


Example 2

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

Sol: Step 2 Calculate  $X_B$  (Public Component of B)

$$\begin{aligned} X_B &= g^b \text{ mod } p \\ &= (17)^4 \text{ mod } 7 \\ &= \end{aligned}$$



$17^1 \text{ mod } 7 = 3$   
 $17^2 \text{ mod } 7 = 2 \checkmark$   
 $17^4 \text{ mod } 7 = 4 \checkmark$

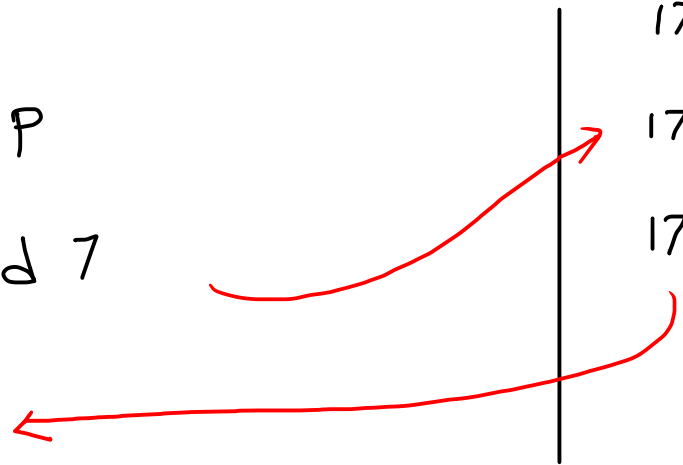
Example 2

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

Sol: Step 2 Calculate  $X_B$  (Public Component of B)

$$\begin{aligned} X_B &= g^b \text{ mod } p \\ &= (17)^4 \text{ mod } 7 \\ &= 4 \end{aligned}$$

$$\begin{aligned} 17^1 \text{ mod } 7 &= 3 \\ 17^2 \text{ mod } 7 &= 2 \checkmark \\ 17^4 \text{ mod } 7 &= 4 \checkmark \end{aligned}$$



∴  $X_A = 1$   
 $X_B = 4$

## Example 2

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

Sol:     Step 3: Calculate Alice's Secret Key

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

## Example 2

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

Sol:     Step 3: Calculate Alice's Secret Key

$$\begin{aligned} A_k &= (X_B)^a \pmod{p} \\ &= (4)^6 \pmod{7} \\ &= \end{aligned}$$

$$\begin{aligned} (4)^1 \pmod{7} &= 4 \\ 4^2 \pmod{7} &= 2 \\ 4^4 \pmod{7} &= 4 \end{aligned}$$

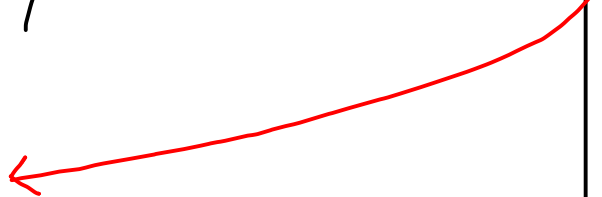
Example 2

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

Sol: Step 3: Calculate Alice's Secret Key

$$\begin{aligned} A_k &= (X_B)^a \pmod p \\ &= (4)^6 \pmod 7 \\ &= 1 \end{aligned}$$

	$(4)^1 \pmod 7 = 4$
}	$4^2 \pmod 7 = 2 \checkmark$
	$4^4 \pmod 7 = 4 \checkmark$
<hr/>	
	$4^6 \pmod 7 = (2 \times 4) \pmod 7$



## Example 2

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

Sol: Step 4: Calculate Bob's Secret Key

$$\begin{aligned} B_K &= (X_A)^b \pmod{p} \\ &= (1)^4 \pmod{7} \\ &= 1 \end{aligned}$$

## Example 2

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

Sol: Step 4: Calculate Bob's Secret Key

$$\begin{aligned} B_K &= (X_A)^b \pmod p \\ &= (1)^4 \pmod 7 \\ &= 1 \end{aligned}$$

∴ Shared Secret Key

$$A_K = B_K = 1$$

### Example 3

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

---

Sol: Step 1: Calculate  $X_A$  (Public Component of Alice)

$$\begin{aligned} X_A &= g^a \text{ mod } p \\ &= (3)^{97} \text{ mod } 353 \\ &= \end{aligned}$$

Calculations



### Example 3

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

---

Sol: Step 2: Calculate  $X_B$  (Public Component of Bob)

$$= g^b \text{ mod } p$$

$$= (3)^{233} \text{ mod } 353$$

=

Calculations

### Example 3

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

---

Sol: Step 3: Calculate Alice's Secret key

$$\begin{aligned} A_K &= (X_B)^a \pmod p \\ &= ( \quad )^{97} \pmod{353} \\ &= \end{aligned}$$

Calculations

### Example 3

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

---

Sol: Step 4: Calculate Bob's Secret key

$$\begin{aligned} B_K &= (XA)^b \pmod p \\ &= ( )^{233} \pmod{353} \\ &= \end{aligned}$$

Calculations

### Example 3

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

---

Sol: Step 5: Shared Secret key —

Calculations

Example: 4

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

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

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

Sol: Step 1: Calculate  $X_A$

$$\begin{aligned} X_A &= g^a \pmod{p} \\ &= 2^9 \pmod{11} \end{aligned}$$

Calculations

Example: 4

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

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

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

Sol: Step 2: Calculate  $X_B$

$$\begin{aligned} X_B &= g^b \pmod{p} \\ &= 2^3 \pmod{11} \end{aligned}$$

Calculations

Example: 4

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

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

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

Sol: Step 3: Calculate A's Secret key

$$\begin{aligned} A_K &= (X_B)^a \pmod p \\ &= ( )^9 \pmod{11} \end{aligned}$$

Calculations

Example: 4

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

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

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

Sol: Step 4 : Calculate B's Secret key

$$\begin{aligned} B_k &= (X_A)^b \pmod p \\ &= ( )^3 \pmod{11} \end{aligned}$$

Calculations



Example: 4

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

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

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

Sol: Step 5: Shared Secret Key

Calculations