Diffie-Hellman Key Exchange

The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values.

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing **discrete logarithms**.

We can define the **discrete logarithm** in the following way.

First,

Let p= prime number

a= primitive root of p

We define a **primitive root** of a prime number *p* as one whose powers modulo *p* generate all the integers from 1 to *p* -1. That is, if *a* is a primitive root of the prime number *p*, then the numbers

$$a \bmod p, a^2 \bmod p, \ldots, a^{p1} \bmod p$$

are distinct and consist of the integers from 1 through *p*- 1 in some permutation.

For any integer *b* and a primitive root *a* of prime number *p*, we can find a unique exponent *i* such that

$$b \equiv a^i \pmod p \text{ where } 0 \leq i \leq (p-1)$$

The exponent *i* is referred to as the discrete logarithm of *b* for the base *a*, mod *p*. We express this value as

$$\mathbf{d\ log}_{a,p}\ (b)$$

The Algorithm:

- There are two publicly known numbers: a prime number *q* and an integer that is a primitive root of *q*.
- Suppose the users A and B wish to exchange a key.

User A selects a random integer $X_A < q$. and computes:

$$Y_A = \alpha^{X_A} \bmod q$$

Similarly, **user B** independently selects a random integer $X_B < q$ and computes:

$$Y_B = \alpha^{X_B} \bmod q$$

- Each side keeps the *X* value private and makes the *Y* value available publicly to the other side.
- User A computes the key as:

$$K = (Y_B)^{X_A} \bmod q$$

and user B computes the key as:

$$K = (Y_A)^{X_B} \bmod q.$$

Calculations produce identical results:

$$K = (Y_B)^{X_A} \bmod q$$

$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q$$

$$= (\alpha^{X_B})^{X_A} \bmod q \qquad \text{by the rules of modular arithmetic}$$

$$= (\alpha^{X_B X_A} \bmod q$$

$$= (\alpha^{X_A})^{X_B} \bmod q$$

$$= (\alpha^{X_A} \bmod q)$$

$$= (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$

$$= (Y_A)^{X_B} \bmod q$$

The figure below shows **The Diffie-Hellman Key Exchange Algorithm**

Global Public Elements

q	prime number
α	$\alpha < q$ *and* α a primitive root of q

User A Key Generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$

Calculation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$

$K = (Y_B)^{X_A} \bmod q$

Calculation of Secret Key by User B

$K = (Y_A)^{X_B} \bmod q$

Calculation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$

The result is that the two sides have exchanged a secret value. Furthermore, because X_A and X_B are private, an adversary only has the following ingredients to work with: q, a, Y_A, and Y_B. Thus, the adversary is forced to take a discrete logarithm to determine the key.

For example,

To determine the private key of user B, an adversary must compute:

$$X_B = \mathrm{dlog}_{\alpha,q}\,(Y_B)$$

The adversary can then calculate the key K in the same manner as user B calculates it.

The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible.

Example:

- p = 11 and a=2
- User A choose XA=9 and calculate:

$YA = a^{XA} mod\ P$

$YA = 2^9 mod\ 11 = 6$ was transmitted to B

- User B choose XB=4 and calculate:

$YB = a^{XB} mod\ P$

$YB = 2^4 mod\ 11 = 5$ was transmitted to A

- After exchange public keys ,each can compute the common secret key by:

A ---------- $K = (YB)^{XA} mod\ p$

$K = 5^9 mod\ 11 = 9$

B ---------- $K = (YA)^{XB} mod\ p$

$K = 6^4 mod\ 11 = 9$

Example:

- p = 353 and a=3
- User A choose XA=97 and calculate

  $YA = a^{XA} mod\ P$

  $YA = 3^{97} mod\ 353 = 40$ was transmitted to B

- User B choose XB=233 and calculate:

  $YB = a^{XB} mod\ P$

  $YB = 3^{233} mod\ 353 = 248$ was transmitted to A

- After exchange public keys ,each can compute the common secret key by:

A ---------- $K = (YB)^{XA} mod\ p$

$K = 248^{97} mod\ 353 = 160$

B ---------- $K = (YA)^{XB} mod\ p$

$K = 40^{233} mod\ 353 = 160$

Example:

- p = 17 and a=3
- User A choose XA=15 and calculate:

$YA = a^{XA} mod\ P$

$YA = 3^{15} mod\ 17 = 6$ was transmitted to B

- User B choose XB=13 and calculate:

$YB = a^{XB} mod\ P$

$YB = 3^{13} mod\ 17 = 12$ was transmitted to A

- After exchange public keys ,each can compute the common secret key by:

A ---------- $K = (YB)^{XA} mod\ p$

$K = 12^{15} mod\ 17 = 10$

B ---------- $K = (YA)^{XB} mod\ p$

$K = 6^{13} mod\ 17 = 10$

Example:

- p = 19 and a=7
- User A choose XA=4 and calculate:

  $YA = a^{XA} mod\ P$

  $YA = 7^4 mod\ 19 = 7$ was transmitted to B

- User B choose XB=8 and calculate:

  $YB = a^{XB} mod\ P$

  $YB = 7^8 mod\ 19 = 11$ was transmitted to A

- After exchange public keys ,each can compute the common secret key by:

A ---------- $K = (YB)^{XA} mod\ p$

$K = 11^4 mod\ 19 = 11$

B ---------- $K = (YA)^{XB} mod\ p$

$K = 7^8 mod\ 19 = 11$

Example:

- p = 23 and a=5
- User A choose XA=6 and calculate:

$YA = a^{XA} mod\ P$

$YA = 5^{6} mod\ 23 = 8$ was transmitted to B

- User B choose XB=15 and calculate:

$YB = a^{XB} mod\ P$

$YB = 5^{15} mod\ 23 = 19$ was transmitted to A

- After exchange public keys ,each can compute the common secret key by:

A ---------- $K = (YB)^{XA} mod\ p$

$K = 19^{6} mod\ 23 = 2$

B ---------- $K = (YA)^{XB} mod\ p$

$K = 8^{15} mod\ 23 = 2$