Primitive root

P=5

	a mod p	a^2 mod p	a^3 mod p	a^4 mod p
a=1	1	1	1	1
a=2	2	4	3	1
a=3	3	4	2	1
a=4	4	1	4	1

2 and 3 are primitive roots of 5

P=7

	a mod p	a^2modp	a^3modp	a^4modp	a^5modp	a^6modp
a=1	1	1	1	1	1	1
a=2	2	4	1	2	4	1
a=3	3	2	6	4	5	1
a=4	4	2	1	4	2	1
a=5	5	4	6	2	3	1
a=6	6	1	6	1	6	1

3 and 5 are primitive roots of 7

Note: Diffie-Helman key exchange algorithm uses this primitive root concept

Shared secret key

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

User B Key Generation

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

Calculation of Secret Key by User A

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

Calculation of Secret Key by User B

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

Figure 10.1 The Diffie-Hellman Key Exchange Algorithm

Example:
Prime No. = 7 (q)
Primitive roots are : 3 and 5.. Will select 5 (r)
Sender private key : 4 (Xa) (It should be less than prime number)
Sender calculate public key Ya as $Ya = r^{Xa} mod\ q$ ===> $Ya=5^4$ mod 7 = 2

Receiver private key Xb=5
Public key of Receiver $Yb = r^{Xb}$ mod q = 5^5 mod 7 = 3

Sahred key from sender side

K1 = Yb^{Xa} mod q = 3^4 mod 7 = 4
K2 = Ya^{Xb} mod q = 2^5 mod 7 = 4

Note:
Xa and Xb are confidential (private keys)
Ya and Yb are public (can be attack by intruder)
Using the values of Ya and Yb it is difficult to get private keys

Discrete Logarithm Problem

$y=a^b \bmod n$
given a, b and n you can easily find y
knowing values of y,a and n it is difficult to find b