1.4 PUBLIC-KEY CRYPTOGRAPHY

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.
- The Diffie-Hellman algorithm uses exponentiation in a finite (Galois) field (modulo a prime or a polynomial)

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

The result is that the two sides have exchanged a secret value.

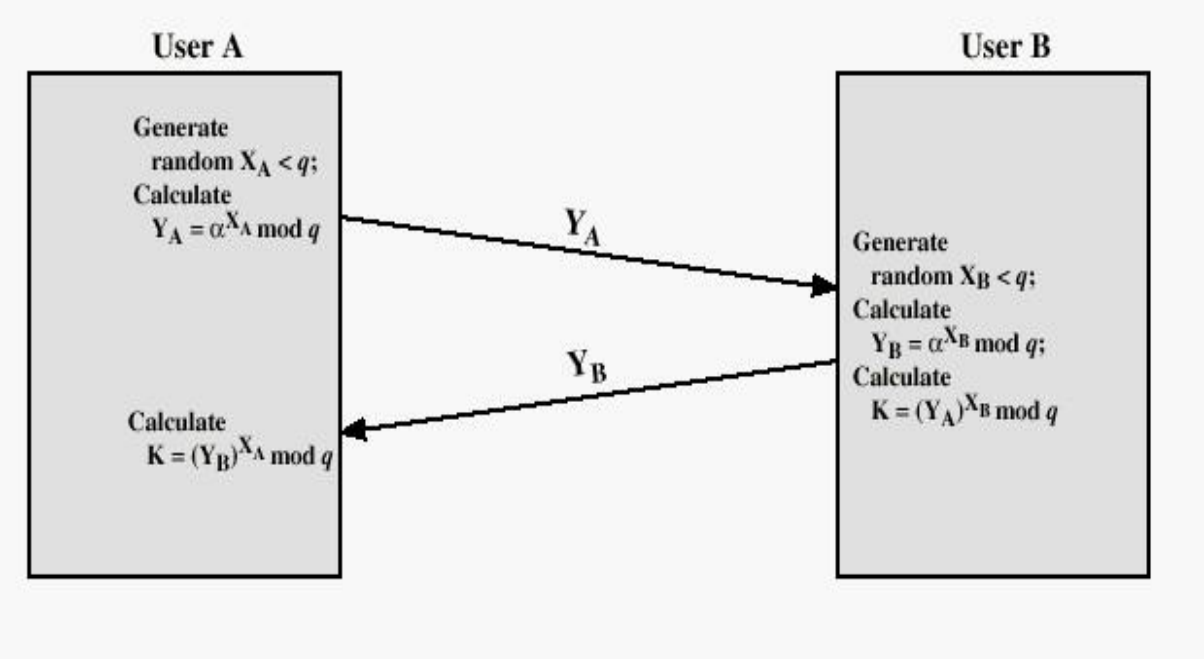
Ex : ὰ = 3 XA = 97 and XB = 233

A computes YA = 397 mod 353 = 40.

B computes YB = 3233 mod 353 = 248.

After they exchange public keys, each can compute the common secret key: A computes K = (YB)XA mod 353 = 24897 mod 353 =160.

B computes K = (YA)XB mod 353 = 40233 mod 353 = 160.



Man-in-the-Middle Attack

Suppose Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows:

1. Alice sends an encrypted message M: E(K2, M).
2. Darth intercepts the encrypted message and decrypts it, to recover M.
3. Darth sends Bob E(K1, M) or E(K1, M'), where M' is any message. In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob.

This vulnerability can be overcome with the use of digital signatures and public-key Certificates.