Information Security
CS3002

Lecture 8
11th September 2024

Dr. Rana Asif Rehman
Email: r.asif@lhr.nu.edu.pk

Asymmetric Cryptography

Diffie-Hellman Algorithm

Diffie-Hellman Key Exchange Algorithm

- First published public-key algorithm.

- A number of commercial products employ this key exchange technique.

- Purpose is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages.

- The algorithm itself is limited to the exchange of secret values.

- Its effectiveness depends on the difficulty of computing discrete logarithms.

Alice

Bob

Alice and Bob share a prime q and α, such that $\alpha < q$ and α is a primitive root of q

Alice and Bob share a prime q and α, such that $\alpha < q$ and α is a primitive root of q

Alice generates a private key X_A such that $X_A < q$

Bob generates a private key X_B such that $X_B < q$

Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$

Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$

Y_A Y_B

Alice receives Bob's public key Y_B in plaintext

Bob receives Alice's public key Y_A in plaintext

Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$

**Bob calculates shared secret key $K = (Y_A)^{X_B} \bmod q$**

Diffie-Hellman key exchange Security

- The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponential modulo a prime, it is very difficult to calculate discrete logarithms.

$$X_B = \text{dlog}_{a,q}(Y_B)$$

- For large primes, the latter task is considered infeasible.

- One way function is different from RSA.

Activity Time
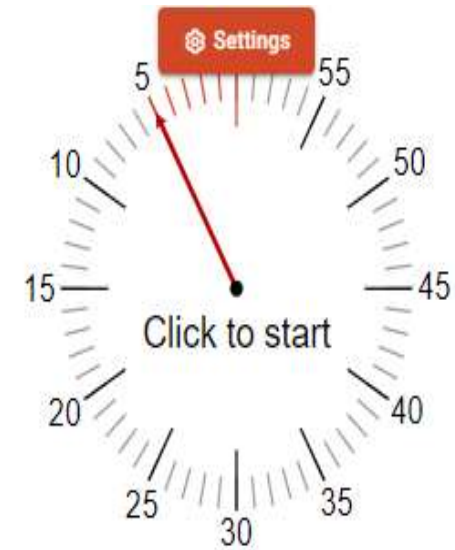
Fine the secret key value by applying the Diffie-Hellman algorithm:

$q = 353$

$\alpha = 3$

$X_A = 97$ (private key of user A)

$X_B = 233$ (private key of user B)

Diffie-Hellman key exchange Example

Here is an example. Key exchange is based on the use of the prime number $q = 353$ and a primitive root of 353, in this case $\alpha = 3$. A and B select private keys $X_A = 97$ and $X_B = 233$, respectively. Each computes its public key:

A computes $Y_A = 3^{97} \bmod 353 = 40$.

B computes $Y_B = 3^{233} \bmod 353 = 248$.

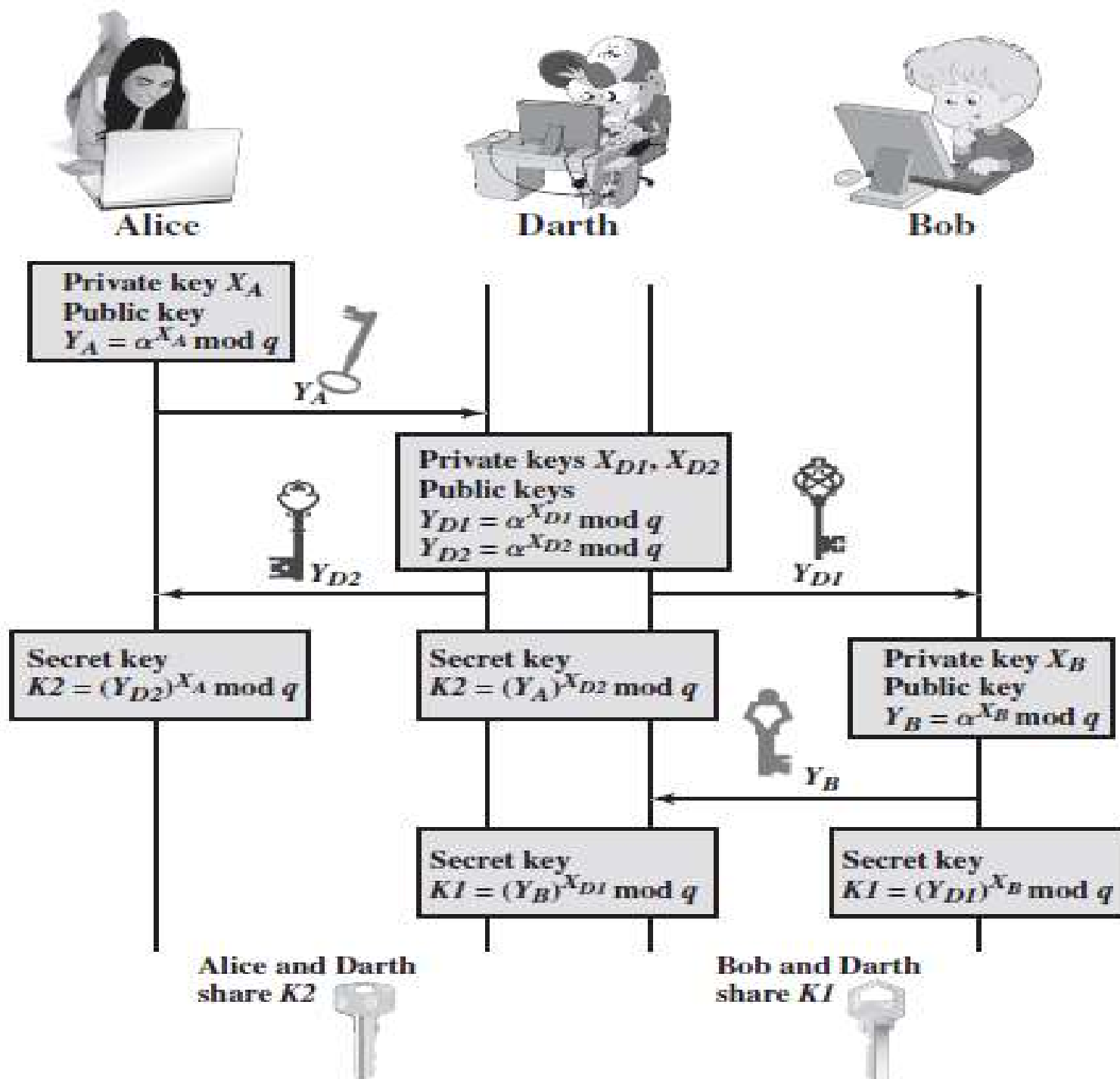After they exchange public keys, each can compute the common secret key:

A computes $K = (Y_B)^{X_A} \bmod 353 = 248^{97} \bmod 353 = 160$.

B computes $K = (Y_A)^{X_B} \bmod 353 = 40^{233} \bmod 353 = 160$.

We assume an attacker would have available the following information:

$$q = 353;\ \alpha = 3;\ Y_A = 40;\ Y_B = 248$$

Man-in-the-Middle Attack

Alice

Darth

Bob

Private key X_A
Public key
$Y_A = \alpha^{X_A} \bmod q$

Y_A

Private keys X_{D1}, X_{D2}
Public keys
$Y_{D1} = \alpha^{X_{D1}} \bmod q$
$Y_{D2} = \alpha^{X_{D2}} \bmod q$

Y_{D2}

Y_{D1}

Secret key
$K2 = (Y_{D2})^{X_A} \bmod q$

Secret key
$K2 = (Y_A)^{X_{D2}} \bmod q$

Private key X_B
Public key
$Y_B = \alpha^{X_B} \bmod q$

Y_B

Secret key
$K1 = (Y_B)^{X_{D1}} \bmod q$

Secret key
$K1 = (Y_{D1})^{X_B} \bmod q$

Alice and Darth
share $K2$

Bob and Darth
share $K1$

9

Man-in-the-Middle Attack (cont.)

1. Darth prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2}.

2. Alice transmits Y_A to Bob.

3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates $K2 = (Y_A)^{X_{D2}} \bmod q$.

4. Bob receives Y_{D1} and calculates $K1 = (Y_{D1})^{X_B} \bmod q$.

5. Bob transmits Y_B to Alice.

6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates $K1 = (Y_B)^{X_{D1}} \bmod q$.

7. Alice receives Y_{D2} and calculates $K2 = (Y_{D2})^{X_A} \bmod q$.

Man-in-the-Middle Attack (cont.)

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key $K1$ and Alice and Darth share secret key $K2$. All future communication between Bob and Alice is compromised in the following way.

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.

The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates;

Solution:

$$Z = E(PU_b, E(PR_a, X))$$
$$X = D(PU_a, E(PR_b, Z))$$