Data Security and Privacy
DSE 3258

L7 –Asymmetric Ciphers

Public-Key Cryptosystems

Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange

- It is a protocol that enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established.
- The purpose of the algorithm 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.
- The Diffie–Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

- This algorithm facilitates the exchange of secret key without actually transmitting it.

Diffie-Hellman Key Exchange

- **Primitive Root:**
- A primitive root of a prime number **p** is defined as one whose powers modulo 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

$$a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p$$

- 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

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

- The exponent **i** is referred to as the **discrete logarithm** of **b** for the base **a**, mod **p**

Diffie-Hellman Key Exchange

- **Primitive roots of value q**
- Example:

  a = 3

  q = 7

  To say a is primitive to q:

  3^1 mod 7 = 3

  3^2 mod 7 = 2

  3^3 mod 7 = 6

  3^4 mod 7 = 4

  3^5 mod 7 = 5

  3^6 mod 7 = 1

Diffie-Hellman Key Exchange

- **Diffie-Hellman Key Exchange Algorithm:**
- For this scheme, there are two publicly known numbers:
- a prime number **q** and an integer **α** that is a primitive root of **q**.
- Suppose the users **A** and **B** wish to exchange a key **K**.
- User **A** selects a random integer $X_A < q$ and computes Y_A.
- Similarly, user **B** independently selects a random integer $X_B < q$ and computes Y_B.
- Each side keeps the **X** value private and makes the **Y** value available publicly to the other side. The whole algorithm can be summarized as follows:

Diffie-Hellman Key Exchange

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

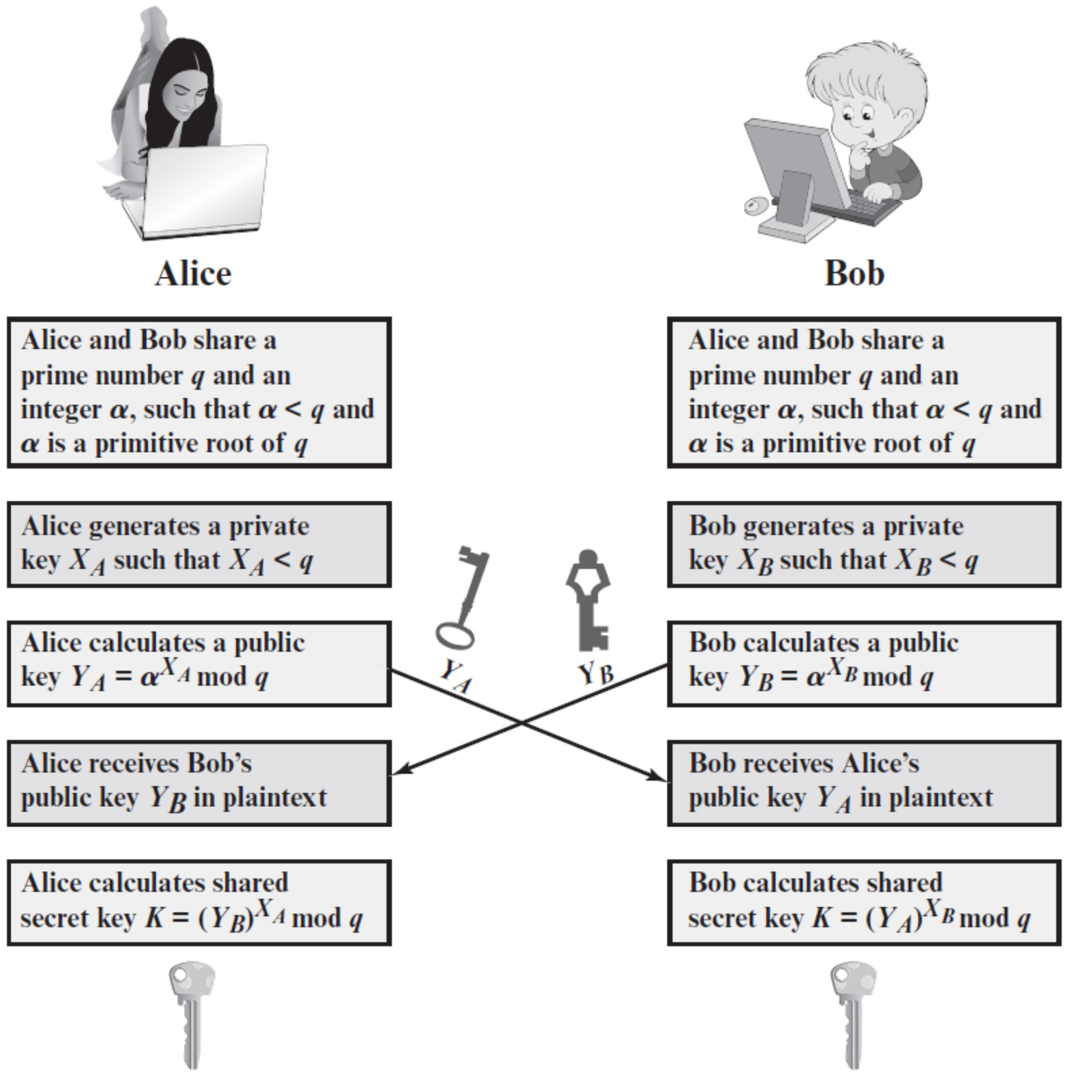
$K = (Y_A)^{XB} \bmod q$

Diffie-Hellman Key Exchange Algorithm

Diffie-Hellman Key Exchange

- **Key Exchange Protocol**

Scenario using Diffie-Hellman:



Diffie-Hellman Key Exchange

- **Diffie-Hellman Key Exchange Example:**
- Key exchange is based on the use of the prime number **q=353** and a primitive root of 353, in this case **α=3**. A and B select secret keys **X_A=97**, **X_B=233** respectively. Each computes its public key:

$$\text{A computes } Y_A = 3^{97} \bmod 353 = 40.$$
$$\text{B computes } Y_B = 3^{233} \bmod 353 = 248.$$

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

$$\text{A computes } K = (Y_B)^{X_A} \bmod 353 = 248^{97} \bmod 353 = 160.$$
$$\text{B computes } K = (Y_A)^{X_B} \bmod 353 = 40^{233} \bmod 353 = 160.$$

DH Example

$q=11 \quad \alpha=3$

$X_A = 5$

$Y_A = 3^5 \bmod 11 = 1$

$X_B = 3$

$Y_B = 3^3 \bmod 11 = 27 \bmod 11 = 5$

$K1 = 5^5 \bmod 11 = 1$

$K2 = 1^3 \bmod 11 = 1$

A & B can share 1

Q1. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged?

1.16
2.17
3.18
4.19

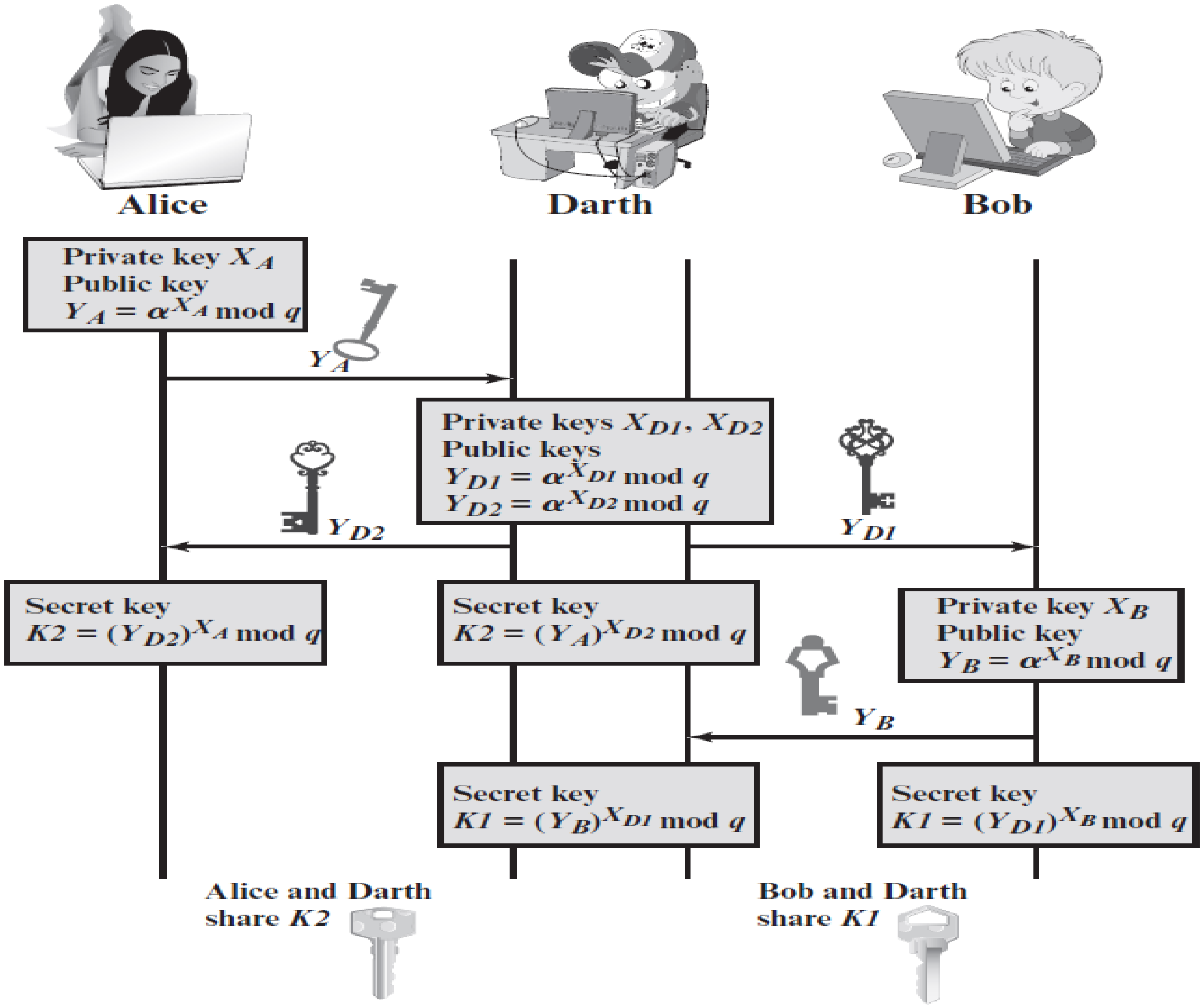
Q2. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 23 and primitive root = 5. If Alice's secret key is 6 and Bob's secret key is 15, what is the secret key they exchanged?

1.4
2.3
3.2
4.1

Breaking of Diffie-Hellman

- The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack.
- In this attack, an opponent Darth intercepts Alice's public value and sends her own public value to Bob.
- When Bob transmits his public value, Darth substitutes it with her own and sends it to Alice.
- Darth and Alice thus agree on one shared key and Darth and Bob agree on another shared key.
- After this exchange, Darth simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party.
- This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants.

Middle man attack / bucket bridge attack



Middle man attack / bucket bridge attack

Alice	Darth	Bob
$q=11 \quad \alpha=7$	$q=11 \quad \alpha=7$	$q=11 \quad \alpha=7$
$X_A = 3$	$M_{XA}=8 \quad M_{XB}=6$	$X_B = 9$
$Y_A = 7^3 \bmod 11$	$Y_A = 7^8 \bmod 11$	$Y_B = 7^9 \bmod 11$
$= 2$	$= 9$	$= 8$
$Y_B = 4$	$Y_B = 7^6 \bmod 11$	$Y_A = 9$
	$= 4$	
$K1 = 4^3 \bmod 11$	$Y_A=2 \quad Y_B=8$	$K2 = 9^9 \bmod 11$
$= 9$	$K1 = 8^8 \bmod 11$	$= 5$
	$= 5$	
	$K2 = 2^6 \bmod 11$	
	$= 9$	