Module 3:
Symmetric Key Cryptography

Dr. Partha Pratim Sarangi
School of Computer Engineering

III. Diffie-Hellman Key Exchange Algorithm

III. Diffie-Hellman Key Exchange Algorithm

- Devised by Whitefield Diffie and Martin Hellman in 1976 for the solution to the key exchange problem.
- This algorithm is used to exchange the secret key between the sender and the receiver.
- This algorithm facilitates the exchange of secret key without actually transmitting it.

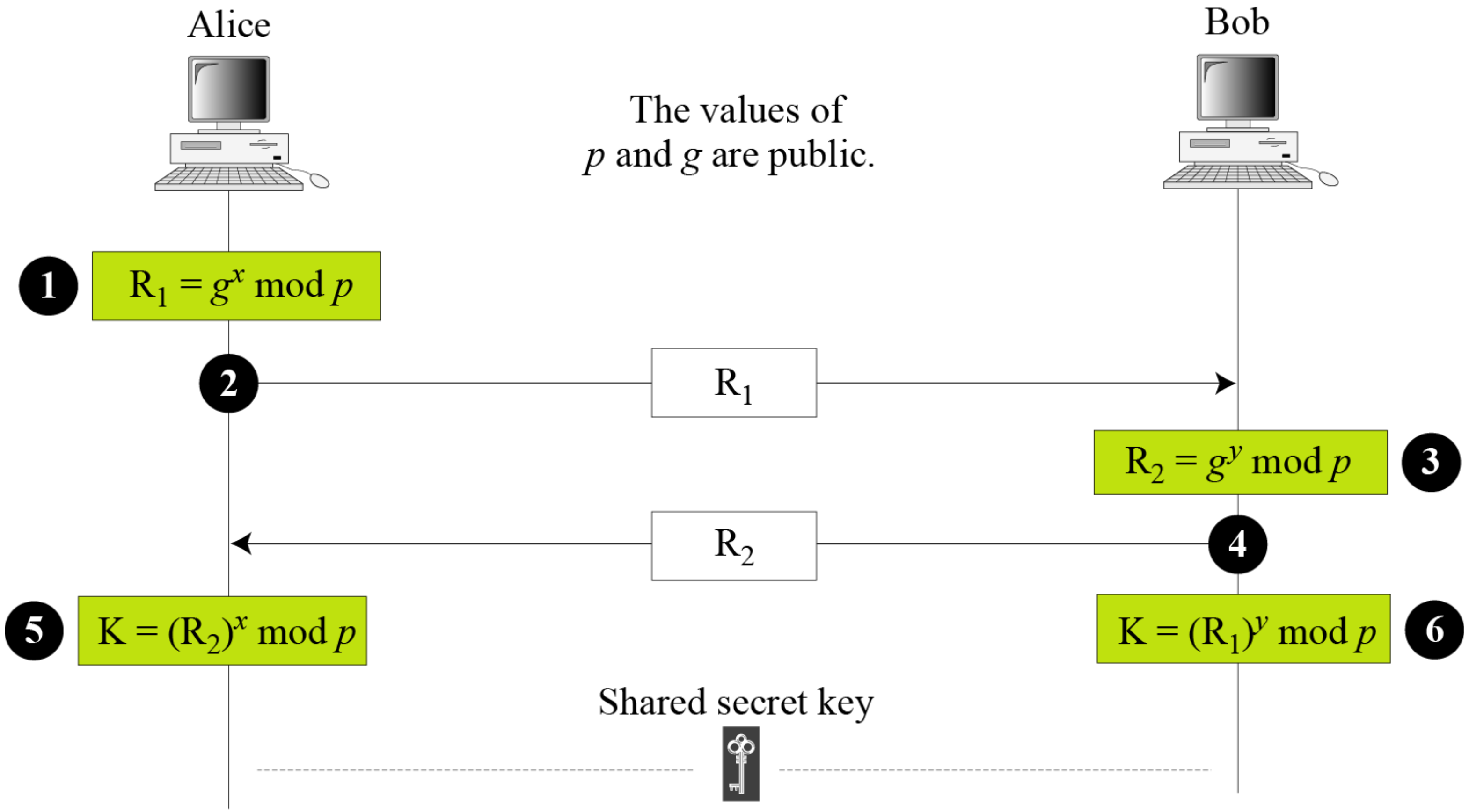
Algorithm:

Two parties choose two large prime numbers n and g, which need not be kept secret

1. Sender(Alice) chooses a large random number x(private key of sender) such that $0 \le x \le n-1$ and calculates $R_1 = g^x \bmod p$
2. Alice sends A to Bob.
3. Receiver(Bob) chooses another large random number y (private key of receiver) such that $0 \le y \le n-1$ and calculates $R_2 = g^y \bmod p$
4. Similarly, Bob sends B to Alice
5. Alice calculates secret key $K=(R_2)^x \bmod p$
6. Bob calculates secret key $K= (R_1)^y \bmod p$

Contd..

Diffie-Hellman Key Exchange



$$K = g^{xy} \bmod p$$

The symmetric (shared) key in the Diffie-Hellman method is $K = g^{xy} \bmod p$.

Example of Diffie Hellman Key Exchange

Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is ?

Solution:

Given: modulus= p = 7

Primitive root=g = 3

Private key of A = x=2

Private key of B = y= 5

Step-01:

Both the parties calculate the value of their public key and exchange with each other.

Public key of A(R_1) $= g^x \bmod p = 3^{\text{private key of A}} \bmod 7$

$= 3^2 \bmod 7$

$= 2$

Public key of B(R_2) $= g^y \bmod p = 3^{\text{private key of B}} \bmod 7$

$= 3^5 \bmod 7$

$= 5$

Example of Diffie Hellman Key Exchange contd..

Step-02:

Both the parties calculate the value of secret key at their respective side.

Secret key obtained by A (K) $= (R_2)^x \bmod p = 5^{\text{private key of A}} \bmod 7$

$= 5^2 \bmod 7$

$= 4$

Secret key obtained by B (K) $= (R_1)^y \bmod p = 2^{\text{private key of B}} \bmod 7$

$= 2^5 \bmod 7$

$= 4$

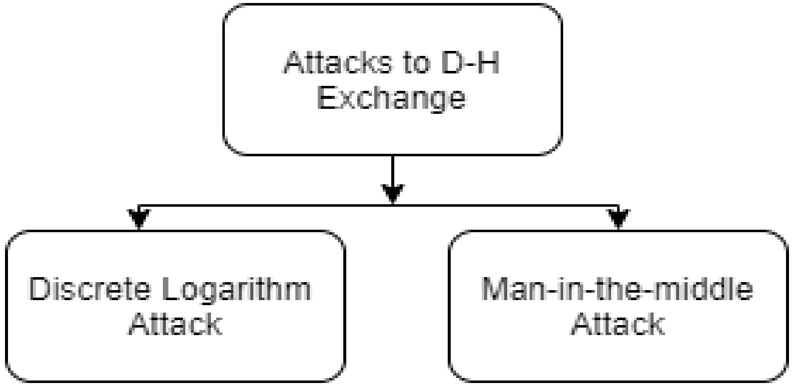
The value of K is the same for both Alice and Bob;

$$\mathbf{g^{xy} \bmod p = 3^{2*5} \bmod 7 = 4.}$$

Finally, both the parties obtain the same value of secret key.

The value of common secret key = 4.

Security of Diffie-Hellman Key Exchange:



Diffie-Hellman key exchange is susceptible to two attacks:

1. Discrete Algorithm Attack
2. Man-in-the-middle attack

1. Discrete Logarithm Attack:

- **Eve, the intruder can intercept R_1 and R_2. If she can find (x) from R_1=g^x mod p and (y) from R_2= g^y mod p, then she calculates the symmetric key = g^{xy} mod p.**

[see next slide for discrete logarithm in details]

Discrete Logarithm

- Consider the finite, multiplicative group(Z_p*,*$_p$),where p is prime. Let g be generator of the group. So,

  g_1 mod p, g_2 mod p…,g_{p-1} mod p

  is a rearrangement of the integers in Z_p.

- Let x be an element in {0,1,2…p-2}. The function

  $y=g^x$ (mod p)

  is referred to as **modular exponentiation** with base **g** and modulus **p.**

- The inverse operation is expressed as :

  $x=\log_g y$(mod p)

  and is referred to as **discrete logarithm.**

  It involves computing x given the values of p, g, y $\in Z_p^*$

$\log y = x \log g \pmod p$

$(\log y/\log g) \pmod p = x$

$\mathbf{\log_g y \pmod p = x}$

Example of discrete logarithm

Compute discrete logarithm in <Z_{11}*,*$_{11}$> for g=2

X	g^x mod 11=y
1	2^1 mod 11 =2
2	2^2 mod 11 = 4
3	2^3 mod 11 =8
4	2^4 mod 11 = 5
5	2^5 mod 11 =10
6	2^6 mod 11 =9
7	2^7 mod 11 =7
8	2^8 mod 11 = 3
9	2^9 mod 11 =6
10	2^{10} mod 11 =1

y	Discrete logarithm $x=\log_2 y \pmod{11}$
1	10
2	1
3	8
4	2
5	4
6	9
7	7
8	3
9	6
10	5

Safe from discrete logarithm attack

To make Diffie-Hellman safe from the discrete logarithm attack, the following are recommended.

a) The prime p must be very large(more than 300 decimal digits).

b) The prime p must be chosen such that p-1 has at least one large prime factor(more than 60 decimal digits).

c) The generator must be chosen from the group <Z_{p*},× >

d) Bob and Alice must destroy x and y after they have calculated the symmetric key. The values of x and y must be used only once.

2. Man-in-the-Middle Attack:

Eve can fool Alice and Bob by creating 2 keys: one between herself and Alice & another between herself and Bob .

a) Alice chooses x, calculates $R_1 = g^x \bmod n$ and sends R_1 to Bob.

b) Eve, the intruder intercepts R_1. She chooses z, calculates $R_2 = g^z \bmod n$ and sends R_2 to both Alice and Bob

c) Bob chooses y, calculates $R_3 = g^y \bmod n$ and sends R_3 to Alice. But, R_3 is intercepted by the Eve and never reaches Alice.

d) Alice and Eve calculates $K_1 = g^{xz} \bmod n$, which becomes a shared key between Alice and Eve. Alice, however, thinks that it is a key shared between Bob and herself.

e) Bob and Eve calculates $K_2 = g^{zy} \bmod n$, which becomes a shared key between Eve and Bob. Bob, however, thinks that it is a key shared between Alice and herself.

2. Man-in-the-Middle Attack contd..: