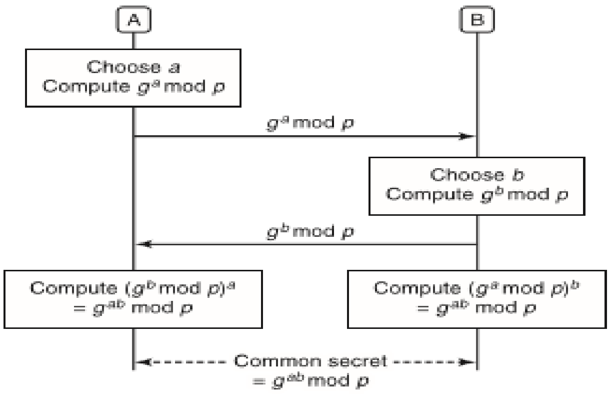
MODULE 2-CHAPTER 3

Steps involved in Diffie Hellman Exchange Protocol

Let A and B are parties to communicate

large prime no- p and generator- g

- A chooses random number **a,** such that, $1<a<p-1$
  Computes Partial key g^amod p and send this to B
- B chooses random number **b,** such that, $1<b<p-1$
  Computes Partial key g^bmod p and send this to A
- On receipt of A's message B computes $(g^a \text{mod } p)^b = g^{ab}$mod p
- On receipt of B's message A computes $(g^b \text{mod } p)^a = g^{ab}$mod p
- g^{ab}mod p is common secret key for A and B to communicate.



Man-in-the middle attack on Diffie-Hellman Key exchange protocol

An attacker C choose secret c and computes g^c mod p

C Intercept A's message to B, substitute it with g^c mod p and send this to B

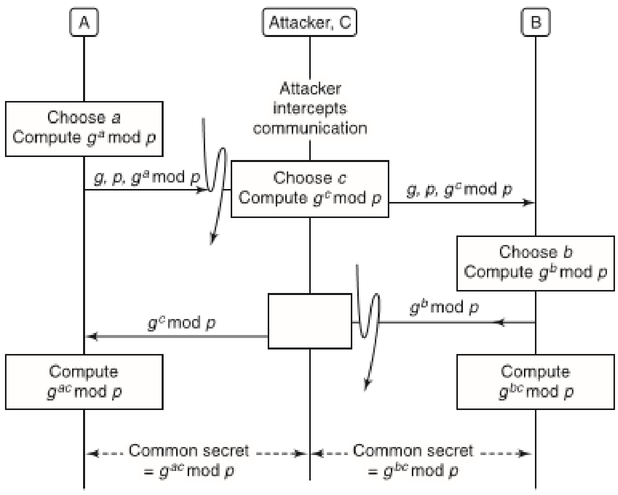
B computes $(g^c \text{ mod } p)^b$ mod p= g^{bc} mod p

C also intercept B's message to A sending g^c mod p

A computes $(g^c \text{ mod } p)^a$ mod p=g^{ac} mod p

C also computes two secrets

g^{bc} mod p and g^{ac} mod p



Steps involved in El Gamal Encryption

Let **A** and **B** are parties to communicate.

Let large prime no- **p** and generator- **g**

- A chooses random number **a** which is its privite key such that, **1<a<p-1**
- Public key of **A** is - **triplet (p, g, α)**

Where $\alpha = g^a \bmod p$

To encrypt the message **M, B** does the following operation

- Chooses a random number **r, 1<r<p-1**
- **Computes**

$$C_1 = g^r \bmod p$$

$$C_2 = (M * \alpha^r) \bmod p$$

Sends **C_1, C_2 to A**

A decrypts the cipher text **C1 and C2** using private key **a**

$(C_1^{-a}) * C_2 \bmod p$

Problems on Diffie-Hellman key exchange technique

1. Find secret using Diffie-Hellman key exchange technique with a common prime q=11 and a primitive root g=2. A has the private key X_A=8, B has the private key X_B=4.

A's public key=g^{XA}mod q =2^8 mod 11=3 Shared secret key= $(g^{XB}\text{mod } q)^{XA}$ mod q =5^8 mod 11 =4	B's public key = g^{XB}mod q =2^4 mod 11=5 Shared secret key= $(g^{XA}\text{mod } q)^{XB}$ =3^4 mod 11 =4

Shared secret key=4

2. Find secret using Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root g=7. A has the private key X_A=5, B has the private key X_B=12.

A's public key=g^{XA}mod q =7^5 mod 71=51 Shared secret key= $(g^{XB}\text{mod } q)^{XA}$ mod q =4^5 mod 71 =30	B's public key = g^{XB}mod q =7^{12} mod 71=4 Shared secret key= $(g^{XA}\text{mod } q)^{XB}$ mod q =51^{12} mod 71 =30

Shared secret key=30

3. Find secret using Diffie-Hellman key exchange technique with a common prime q=131 and a primitive root g=2. A has the private key X_A=24, B has the private key X_B=17.

A's public key=g^{XA}mod q =2^{24} mod 131=46 Shared secret key= $(g^{XB}\text{mod q})^{XA}$ mod q =72^{24} mod 131 =13	B's public key = g^{XB}mod q =2^{17} mod 131=72 Shared secret key= $(g^{XA}\text{mod q})^{XB}$ mod q =46^{17}mod 131 =13

Shared secret key=13

Note when exponent is higher value following method can be applied.

Convert exponent into binary form, then apply the steps

1. Initially d=1
2. consider binary form exponent from left to right

   If bit=0

   Compute d^2 mod p

   d = d^2 mod p

   If bit=1

   Compute d^2 *b mod p ((d^2mod p) * b mod p)

   d = d^2 *b mod p

In above example, to compute 72^{24} mod 131 above method can be applied
Binary of exponent 24 is 1 1 0 0 0

b = 72, q=131

Assume d=1	1	1	0	0	0
d	1	72	29	55	12
d^2 mod q	1	75	55	12	13 (Ans)
d^2b mod q	72	29			

72^{24} mod 131=13

In above example, to compute 46^{17}mod 131 above method can be applied
Binary of exponent 17 is 1 0 0 1

b = 46, q=131

Assume d=1	1	0	0	0	1
d	1	46	20	7	49
d^2 mod q	1	20	7	49	43
d^2b mod q	46				13 (Ans)

Problems on El Gamal Encryption

1. Common prime p=19 and g=10. A's private key, a= 5, B choose random integer r=6, message M=17
    b. Compute public key of A
    c. B perform encryption for the message M=17, Compute cipher text C_1 and C_2
    d. Decryption of C_1 and C_2 by A

Solution

A's corresponding public key- **α(alpha)**

$\alpha = g^a \bmod p = 10^5 \bmod 19 = \mathbf{3}$

If B perform encryption for the message M=17.

Compute C_1 and C_2

$C_1 = g^r \bmod p$

$= 10^6 \bmod 19 = \mathbf{11}$

$K = \alpha^r \bmod p = 3^6 \bmod 19 = \mathbf{7}$

$C_2 = (K*M) \bmod p$

$= (7*17) \bmod 19 = \mathbf{5}$

Encrypted two cipher text are $\mathbf{C_1=11, C_2=5}$

A Decrypt the Cipher $\mathbf{C_1}$ **and** $\mathbf{C_2}$ using private key **a** and obtain the message **M**.

$K = (C_1)^a \bmod p$

$= 11^5 \bmod 19 = \mathbf{7}$

$M = (C_2 K^{-1}) \bmod p$

$= (C_2 * K^{-1} \bmod p) \bmod p$

$= 5 * 11 \bmod 19 = \mathbf{17}$

M =17

$(C_2 K^{-1}) \bmod p$ can be written as

$(C_2 * K^{-1} \bmod p) \bmod p$

K =7

$K^{-1} \bmod p = 7^{-1} \bmod 19$

=11 this obtained as follows

$7*1 \bmod 19 \neq 1$

$7*2 \bmod 19 \neq 1$

-

-

$7*11 \bmod 19 = 1$

3. Common prime p=131 and g=2. A's private key, a= 97, B choose random integer r=33, message M=17
   a. Compute public key of A
   b. B perform encryption for the message M=17, Compute cipher text C_1 and C_2
   c. Decryption of C_1 and C_2 by A

El Gamal Encryption common prime p=131 and g=2.

a) A's private key, a= 97, corresponding public key α (alpha)

   $\alpha = g^a \bmod p$

   $= 2^{97} \bmod 131 = 14$

   $\boldsymbol{\alpha = 14}$

b) B choose random integer **r=33**,

   If B perform encryption for the message **M=75**,

   Compute C_1 and C_2.

   $C_1 = g^r \bmod p = 2^{33} \bmod 131 = 103$

   $K = \alpha^r \bmod p = 14^{33} \bmod 131 = 95$

   $C_2 = K{*}M \bmod p = 95{*}75 \bmod 131 = 51$

c) Decrypt the Cipher C_1 and C_2 and obtain the message M.

   $K = (C_1)^a \bmod p = 103^{97} \bmod 131 = 95$

   $M = (C_2\, K^{-1}) \bmod p = 51 {*}(95^{-1} \bmod 131) \bmod 131$

   $M = (51 * 40) \bmod 131 = 75$

$95^{-1} \bmod 131 = 40$ (apply extended Euclidean algorithm)

In above example, to compute $2^{97} \bmod 131$ above method can be applied

Binary of exponent 97 is 1 1 0 0 0 0 1

b = 2, q=131

Assume d=1	1	1	0	0	0	0	1
d	1	2	8	64	35	46	20
$d^2 \bmod q$	1	4	64	35	46	20	7
$d^2b \bmod q$	2	8					14(Ans)

$14^{33} \bmod 131$

Binary of exponent 33 is 1 1 0 0 0 0 1

b = 14, q=131

Assume d=1	1	0	0	0	0	1
d	1	14	65	33	41	109
$d^2 \bmod q$	1	65	33	41	109	91
$d^2b \bmod q$	14					95(Ans)