ElGamal Cryptosystem

System design level

- **All users agree on a large prime *p* and a *generator g*;**
- **Users *A, B,*…select their private keys *a, b,*…;**
- **Every user generates her/his public key**

$$P_a = g^a \bmod p; \quad P_b = g^b \bmod p; \ldots$$

- **System parameters *p* and *g* are known to all users;**
- **Public keys are known to all users.**

Protocols of Communication

{*A* sends message *m*<*p* to *B*}

Encryption protocol {*A*'s actions}

1. Selects randomly *secret* key *k*;

2. Computes $M := \left[P_b\right]^k \bmod p$ **(mask);**

3. Computes $C := (mM) \bmod p$ **(ciphertext);**

4. Computes $H := g^k \bmod p$ **(hint);**

5. Sends {*C, H*} to *B* over Internet

Decryption protocol {B computes}

6. Using his private key *b* $q := p-1-b$;

7. $R := H^q \bmod p$; **(opener);**

8. $D := (CR) \bmod p$;

Property: $\boxed{D=m}$

Solution process

1. Find the public keys for *A* and *B*;

2. Compute the *mask*;

3. Compute the *ciphertext*;

4. Compute the *hint*;

5. Show how *B* is de-masking the ciphertext.

***Example*1:**

- **Select *p*=53, find the smallest generator *g*;**
- **Select *a*=9, *b*=13 and *A*'s secret key *k*=8;**
- **Encrypt and decrypt message *m*=21.**

Solution:

$52 = 13^1 * 2^2$

3 is a generator

g = 3;

k = 8; *a*=9, *b*=13; *p*=53; *m*=21

Bob:

$Pb = 3^{13} \bmod 53 = 30;$

Alice:

$M = 30^8 \bmod 53 = 1 \bmod 53$ – BAD CHOICE!

Choose a different k:

k = 17;

$M = 30^{17} \bmod 53 = 30;$

$C = (21*30) \bmod 53 = 47;$

$H = g^k = 3^{17} = 45;$

Alice sends to Bob: 47; 45

Bob:

$R := 45^{53-1-13} \bmod 53 = 23$

$D := 47*23 \bmod 53 = 21$