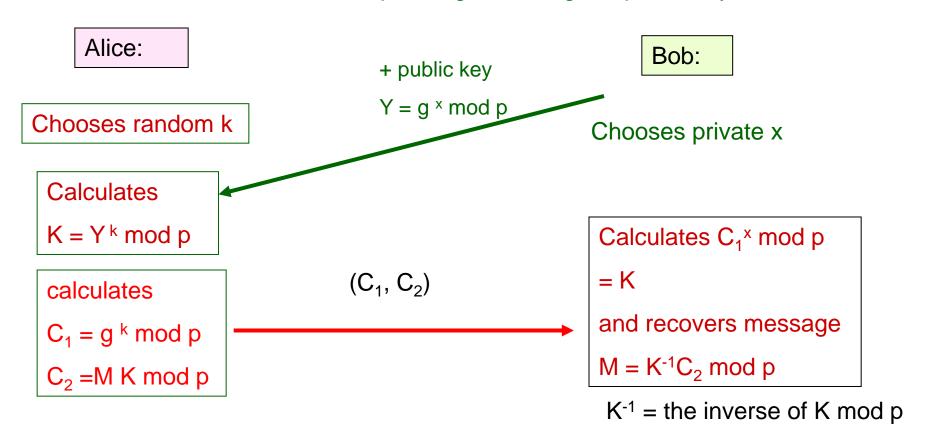
## Elgamal encryption algorithm

Prime p and generator g are public keys of Bob



Elgamal = Diffie Hellman key exhange + encryption by multiplying mod p

## Elgamal example

Alice sends a message M = 100 to Bob

Prime p = 139 and g = 3

Alice:

public key

 $44 = 3^{12} \mod 139$ 

Bob:

Chooses k = 52

Chooses private x = 12

Calculates

 $K = 44^{52} \mod 139 = 112$ 

**Calculates** 

$$C_1 = 3^{52} \mod 139 = 38$$

 $C_2 = 100*112 \mod 139 = 80$ 

 $(C_1, C_2)=(39,80)$ 

Calculates K =  $38^{12}$  mod 139 = 112

 $K^{-1} = 112^{-1} \mod 139 = 36$ 

and recovers message

 $M = K^{-1}C_2 \mod p =$ 

 $36*80 \mod 139 = 100$ 

Elgamal = Diffie Hellman key exhange + encryption by multiplying mod p

## Elgamal security

- Each user has a private key x
- Each user has three public keys: prime modulus p, generator g and public Y = g<sup>x</sup> mod p
- Security is based on the difficulty of DLP
- Secure key size > 1024 bits (today even 2048 bits)
- Elgamal is quite slow, it is used mainly for key authentication protocols
- Now widely used, but Elliptic Curve variant is increasingly popular