

# The ElGamal Cryptosystem

- The security of the RSA cryptosystem is based on the difficulty of factoring integer.
- The security of the ElGamal cryptosystem is based on the difficulty of finding discrete logarithms modulo a large prime.

## I. Public key cryptosystem-ElGamal cryptosystem

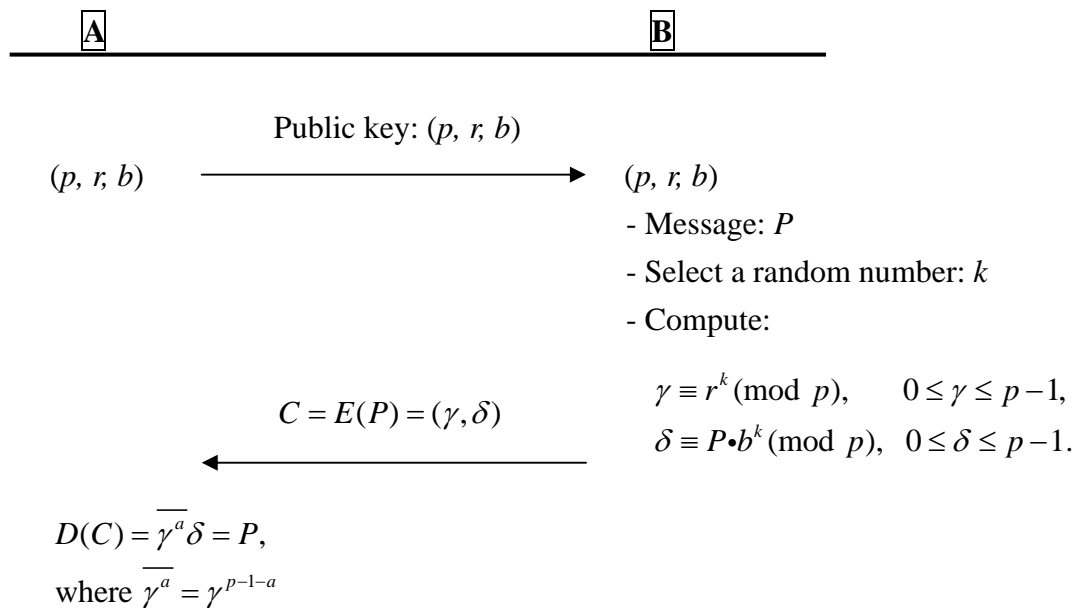
1. **A** select:
  - a prime  $p$
  - a primitive root  $r$  of  $p$
  - an integer  $a$ ,  $0 \leq a \leq p-1$ .

2. **A** compute:

$$b \equiv r^a \pmod{p}, \quad 0 \leq a \leq p-1$$

3. Public key:  $(p, r, b)$   
Private key:  $a$

4. Encrypting and Decrypting a message:



5. Proof:

$$\begin{aligned} D(C) &\equiv \overline{\gamma^a} \delta \pmod{p} \\ &\equiv \overline{r^{ka}} \cdot P b^k \pmod{p} \\ &\equiv \overline{(r^a)^k} P b^k \pmod{p} \\ &\equiv \overline{b^k} P b^k \pmod{p} \\ &\equiv \overline{b^k} b^k P \pmod{p} \\ &\equiv P \pmod{p} \end{aligned}$$

## II. Signing message in the ElGamal cryptosystem

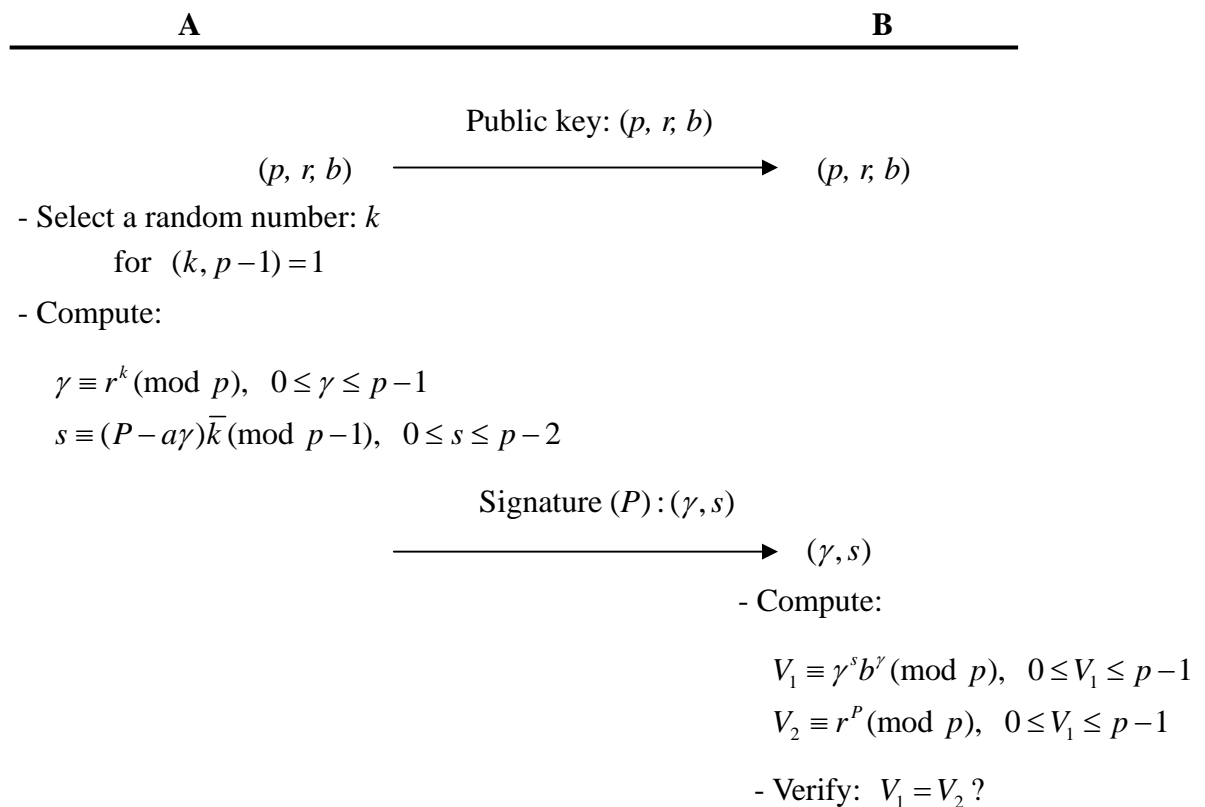
1. **A** select:
  - a prime  $p$
  - a primitive root  $r$  of  $p$
  - an integer  $a$ ,  $0 \leq a \leq p-1$ .

2. **A** compute:

$$b \equiv r^a \pmod{p}, \quad 0 \leq a \leq p-1$$

3. Public key:  $(p, r, b)$   
Private key:  $a$

4. Signing a message:



5. Proof:

$$\begin{aligned}V_1 &\equiv \gamma^s b^\gamma \pmod{p} \\ &\equiv \gamma^{(P-a\gamma)\bar{k}} b^\gamma \pmod{p} \\ &\equiv (\gamma^{\bar{k}})^{P-a\gamma} b^\gamma \pmod{p} \\ &\equiv r^{(P-a\gamma)} b^\gamma \pmod{p} \\ &\equiv r^P \overline{r^{a\gamma}} b^\gamma \pmod{p} \\ &\equiv r^P \overline{b^\gamma} b^\gamma \pmod{p} \\ &\equiv r^P \pmod{p} \\ &= V_2\end{aligned}$$