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, $0 \le a \le p-1$.

2. **A** compute:

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

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

4. Encrypting and Decrypting a message:

Public key: (p, r, b)

(p, r, b) ⟶ (p, r, b)

- Message: P
- Select a random number: k
- Compute:

$$\gamma \equiv r^k \pmod{p}, \qquad 0 \le \gamma \le p-1,$$
$$\delta \equiv P \bullet b^k \pmod{p}, \quad 0 \le \delta \le p-1.$$

$C = E(P) = (\gamma, \delta)$ ⟵

$D(C) = \overline{\gamma^a}\delta = P,$

where $\overline{\gamma^a} = \gamma^{p-1-a}$

5. Proof:

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

II. Signing message in the ElGamal cryptosystem

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

2. **A** compute:

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

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

4. Signing a message:

A		**B**
	Public key: (p, r, b)	
(p, r, b)	$\longrightarrow$	(p, r, b)
- Select a random number: k for $(k, p-1) = 1$		
- Compute: $\gamma \equiv r^k \pmod{p}$, $0 \le \gamma \le p-1$; $s \equiv (P - a\gamma)\bar{k} \pmod{p-1}$, $0 \le s \le p-2$		
	Signature $(P) : (\gamma, s)$ $\longrightarrow$ (γ, s)	
		- Compute: $V_1 \equiv \gamma^s b^\gamma \pmod{p}$, $0 \le V_1 \le p-1$; $V_2 \equiv r^P \pmod{p}$, $0 \le V_1 \le p-1$
		- Verify: $V_1 = V_2$?

5. Proof:

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