ElGamal Cryptosystem

Monday, November 10, 2025 9:45 AM

Recall: DLog
DH assumption

Missing
100 # 1, 4, 6, 7, 1
200 # 1, 7, 24, 27
500 # 2, 4, 14, 19, 21, 26,

§ 10.4 El Gamal Cryptosystem

1] ElGamal Cryptosystem
- Public-key based on DLP / DH assumption
- By Taher ElGamel in 1985

2] El Gamal Setup:
- $\mathbb{Z}_p^*$, with large prime p.
- generator, $\langle g \rangle = \mathbb{Z}_p^*$
- keys:

private-key x
public-key (g, y, p); $y = g^x$

Forouzan notation
e_1 for g
e_2 for y
d for x
pub-key (e_1, e_2, p)
(C_1, C_2) for (a, b)

3] Encryption: Bob wants to encrypt M to Alice with (g, y, p)

① Bob chooses a random r (unique secret)
② Bob computes: $a = g^r$
$b = y^r \cdot M$

③ Bob sends ciphertext: $C = (C_1, C_2) = (a, b)$

4] Decryption: To decrypt $C = (a, b)$

$$M = b \cdot a^{-x}$$

Proof:

$$b \cdot a^{-x} = (y^r \cdot M) \cdot (g^r)^{-x}$$
$$= (g^{xr} \cdot M) \cdot g^{-xr}$$
$$= M$$

$$b = y^r \cdot M$$
$$\Rightarrow M = b \cdot y^{-r}$$
$$= b \cdot (g^x)^{-r}$$
$$= b \cdot g^{-xr}$$
$$= b \cdot a^{-x}$$

5] e.g. $p = 13$, $g = 2$

pri-key: $x = 3$

pub-key: $y = g^x = 2^3 \equiv 8 \pmod{13}$

13
26
39
52
130

encrypt $M = 5$

① Choose $r = 7$

② compute $a = g^r \equiv 2^7 \equiv 11 \pmod{13}$

$$b = y^r \cdot M = 8^7 \cdot 5$$
$$\equiv (2^3)^7 \cdot 5$$
$$\equiv 2^{-3} \cdot 5$$
$$\equiv 8^{-1} \cdot 5$$
$$\equiv 5 \cdot 5 \equiv 12 \pmod{13}$$

③ $C = (11, 12)$

Decrypt $C = (c_1, c_2) = (11, 12)$

$$M = b \cdot a^{-x} \pmod{p}$$

$$\equiv 12 \cdot 11^{-3}$$

$$\equiv (-1)(-2)^{-3}$$

$$\equiv 8^{-1}$$

$$\equiv 5 \pmod{13}$$