El Gamal Encryption

Setup: p (modulus), g (primitive root)] PUBLIC

Alice ---- message ----> Bob

message $0 \le m < p$

permanent { Private key: $0 \le b < p-1$ random
Public key: $B = g^b$ } just like D-H

B

ENCRYPTION

new each time { Ephemeral key pair:
Private: $0 \le k < p$ random
Public: $K = g^k$ } just like D-H

Compute masked message: $c = B^k m$

$B^k = g^{kb} = K^b$
"shared secret"
"mask"

Ciphertext: (K, c) ----------> (K, c)

DECRYPTION

$(K^b)^{-1} c = g^{-kb}(g^{kb} m)$
$= m$

we need to compute inverse

Why does Alice use a new ephemeral key each time?

Sps k is reused. Then

ciphertext #1 $= (K, c_1) = (K, g^{kb} m_1)$

ciphertext #2 $= (K, c_2) = (K, g^{kb} m_2)$

Observation: If we know m_1, then we know $g^{kb} = c_1 m_1^{-1}$

$= g^{kb} m_1 m_1^{-1}$

$\Rightarrow$ then we can decrypt m_2 just like Bob can.

Moral: Use a different ephemeral key each time.

Chinese Remainder Thm (Sunzi's Thm)

Example. $x \equiv 2 \pmod 5$ $\quad x \equiv 3 \pmod 7$

$x = 2 + 5i$ $\quad x = 3 + 7j$

① Linear Diophantine Eqn:

$$7s + 5t = 1$$

Solve: $(s,t) = (3,-4)$

$$\Rightarrow \quad 7s \equiv 1 \pmod 5$$
$$5t \equiv 1 \pmod 7$$

②

$$x = \underbrace{5\_\_\_\_}_{\equiv 3 \pmod 7} + \underbrace{7\_\_\_\_}_{\equiv 2 \pmod 5}$$

want: $\equiv 3 \pmod 7$ $\quad \equiv 2 \pmod 5$

$$= \underbrace{5 \cdot t}_{\equiv 1 \pmod 7} \cdot 3 + \underbrace{7 \cdot s}_{\equiv 1 \pmod 5} \cdot 2$$

want: $\equiv 1 \pmod 7$ $\quad \equiv 1 \pmod 5$

(t = inverse of 5 mod 7) $\quad$ (s = inverse of 7 mod 5)

$$= 5 \cdot (-4) \cdot 3 + 7 \cdot 3 \cdot 2$$

$$= -60 + 42 = -18$$

③ $x \equiv -18 \pmod{5 \cdot 7}$ is solution.

$\equiv 17$

④ Verify $17 \equiv 2 \pmod 5$ ✓

$17 \equiv 3 \pmod 7$ ✓