Lecture 7 Elgamal PKC §2.4.

Recall from end of last time

Elgamal Publically fixed: p a large prime, $g \in \mathbb{F}_p^\times$ a primitive root / generator.

Alice | **Bob**

Pick private key $a \in \mathbb{Z}/(p-1)\mathbb{Z}$

Pub key: $A = g^a \in \mathbb{F}_p^\times$ → A

Publish public key

Encode plaintext $m \in \mathbb{F}_p^\times$.

Pick random $k \in \mathbb{Z}/(p-1)\mathbb{Z}$

Compute $c_1 = g^k \in \mathbb{F}_p$, $c_2 = mA^k \in \mathbb{F}_p^\times$

encrypt

ciphertext is (c_1, c_2).

(c_1, c_2) ←

Compute

$$c_2 \cdot c_1^{-a} = c_2 \cdot g^{-ak} = (mA^k) \cdot A^{-k} = m.$$

decrypt

Ex $g = 2 \in \mathbb{F}_{11}^{\times}$.

Alice | **Bob**

Private key $a = 4 \in \mathbb{Z}/10\mathbb{Z}$

Public key $A = 2^4 = 16 = 5$ $\xrightarrow{A = 5}$

Plaintext $m = 7 \in \mathbb{F}_{11}$

Pick $k = 3 \in \mathbb{Z}/10\mathbb{Z}$

Compute

$c_1 = g^k = 2^3 = 8$

$c_2 = m A^k = 7 \cdot 5^3$

$\equiv 6 \pmod{11}$

$\xleftarrow{(c_1, c_2)}$

$(8, 6)$

Compute

$m = c_2 \cdot c_1^{-a}$

$= 6 \cdot 8^{-4}$

$= 6 \cdot (-4)^4$ b/c $8^{-1} \equiv -4 \pmod{11}$.

$= \cdots$

$= 7 \pmod{11}$

Prop Breaking Elgamal is equal in hardness to breaking the Diffie Hellman problem.

pf ① Elgamal $\leq$ DHP:

If Eve has an oracle to solve DHP, then

WTS Eve can use it to solve Elgamal.

Eve knows: $c_1 = g^k$

$c_2 = mA^k = mg^{ak}$

$A = g^a$

Can solve DHP: given $c_1 = g^k$ & $A = g^a$ she can find g^{ak}. Then from c_2 & g^{ak}, finds $m = c_2 g^{-ak}$. $\leq$ ✓

② $\geq$

Suppose Eve can solve Elgamal. So given $c_1 = g^k$, $c_2 = mA^k$, & $A = g^a$ she can find $m = c_2 \cdot g^{-ak}$

She is given $X = g^x$ & $Y = g^y$ & wants to find g^{xy}.

She can set $c_1 = X$ & $A = Y$ & $c_2 = 1$.

Then she finds $M = 1 \cdot g^{-xy}$.

& so $g^{xy} = M^{-1}$.

□