PUBLIC KEY ENCRYPTION II

El Gamal encryption (review)
Semantic security
IND-CCA2 (ACCA) security
Cramer Shoup PK encryption
RSA

EL GAMAL ENCRYPTION

Public key encryption scheme. Assume DLP, CDH are hard.

$\mathbb{Z}_p^*$ for large random prime p

$SK = x$, $0 \leq x < p-1$

$PK = (p, g, g^x)$

ENCRYPTION Bob does the following

(a) Represent message as integer $m \in \{0, 1, \ldots p-1\}$

(b) Select a random k, $1 \leq k < p-1$

(c) $y = g^k \bmod p$, $\delta = m \cdot (g^x)^k \bmod p$

(d) Send ciphertext $c = (y, \delta)$ to Alice

DECRYPTION To recover plaintext, Alice does

(a) Compute $y^{-x} \bmod p = y^{p-1-x} \bmod p$

(b) Recover $m = \underbrace{(y^{-x})}_{g^{-kx}} \cdot \underbrace{\delta}_{m \cdot g^{kx}} \bmod p$

SEMANTIC SECURITY

- Early def of security for PK encryption (Goldwasser, Micali)
- Adversary can't tell $E(m_0)$ from $E(m_1)$
- Game

$$\begin{array}{lcl} \text{Keygen } (PK, SK) & \xrightarrow{\quad PK \quad} & \text{Adv} \\ & \xleftarrow[m_0 \neq m_1]{m_0, m_1} & \\ \text{pick } b \in_R \{0,1\} & \xrightarrow{\quad E(m_b) \quad} & \\ \underbrace{b = \hat{b}\ ?}_{\text{if yes, adversary wins}} & \xleftarrow{\quad \hat{b} \quad} & \end{array}$$

Scheme is semantically secure if $Pr[\text{Adv wins}] \leq \frac{1}{2} + \varepsilon$

Note: scheme must be randomized to be sem secure

IS EL GAMAL SEMANTICALLY SECURE?

Decision Diffie Hellman (DDH):

Distinguishing (g^a, g^b, g^c) from (g^a, g^b, g^{ab}) is hard
a, b, c random $\quad a, b$ random

Theorem (Tsiounis & Yung):

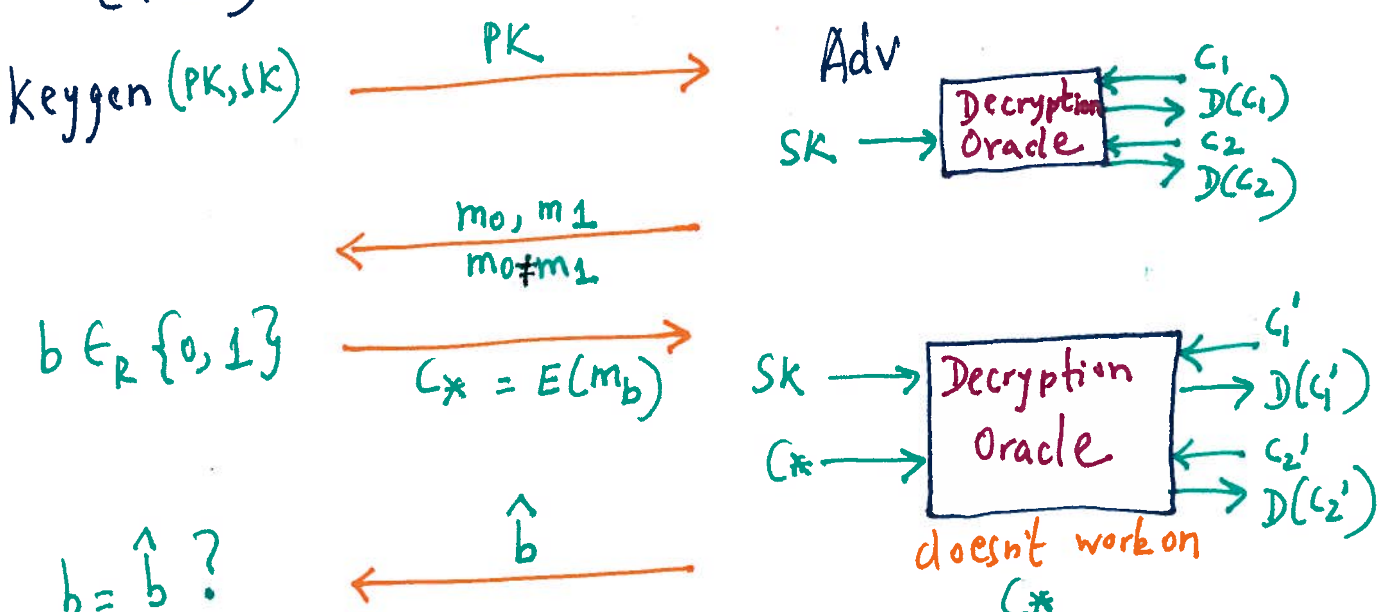
El Gamal is semantically secure $\Leftrightarrow$ DDH holds in G

IND-CCA2 SECURITY

El Gamal is malleable

Given $E(m) = (g^k, m.g^{xk})$
easy to produce $E(2m) = (g^k, 2m.g^{xk})$
without knowing m! (Can outbid you at an auction)

IND-CCA2 (ACCA): Adaptive $\underbrace{\text{chosen ciphertext attacks}}_{\text{non-adaptive : IND-CCA1}}$



if yes, adversary wins

Scheme is IND-CCA2 (ACCA) secure if $Pr[\text{Adv wins}] \leq 1/2 + \varepsilon$

EL Gamal is not IND-CCA2 secure

Given $C_* = (g^k, m.g^{xk})$ ask to decrypt
$C_*' = (g^k, 2mg^{xk}) \Rightarrow 2m \Rightarrow m$ known

Homomorphic : $E(m_1) \cdot E(m_2) = E(m_1 . m_2)$

CRAMER SHOUP

IND-CCA2 secure (can be viewed as an elaboration of El Gamal)

Let G be a cyclic group of prime order q, i.e., every element other than 1 is a generator. (e.g., squares in $\mathbb{Z}_p^*$, where $p = 2q+1$)

Keygen: g_1, g_2 random generators in G

$x_1, x_2, y_1, y_2, z \in_R \{0, 1, .. q-1\}$

H: hash function mapping $G \times G \times G \to \{0, 1, .. q-1\}$

$c = g_1^{x_1} g_2^{x_2}$

$d = g_1^{y_1} g_2^{y_2}$

$h = g_1^{z}$

$PK = (g_1, g_2, c, d, h, H)$

$SK = (x_1, x_2, y_1, y_2, z)$

Encryption, decryption use H and are significantly more complicated than El Gamal – see Wikipedia

Theorem: Cramer Shoup is IND-CCA2 secure if DDH assumption holds in G and H is target collision resistant.

RSA ENCRYPTION

Keygen: p, q random primes

$n = p \cdot q$

$e \in_R \mathbb{Z}^*_{\phi(n)}$ $\qquad \phi(n) = (p-1)(q-1)$

need $\gcd(e, \phi(n)) = 1$

$d = e^{-1} \pmod{\phi(n)}$ $\qquad$ { e can be short, d shouldn't be }

use Extended Euclidean algorithm

$PK = (n, e)$

$SK = (d, p, q)$

FACTORING: Assume it is infeasible for an adversary to produce p, q, given n, where p, q are randomly chosen (768 bit number has been factored in 2010.)

ENCRYPTION: Given $m \in \mathbb{Z}_n$ & $PK = (n, e)$

$c = E(m) = m^e \pmod n$

DECRYPTION: Given c & $SK = (d, p, q)$

$m = D(c) = c^d \pmod n$

p & q should not be too close

$p-1, q-1$ should not have only small prime factors

etc...

CORRECTNESS OF RSA

Chinese Remainder Theorem (CRT): Let $n = p \cdot q$, where p, q are distinct primes.

Then $(\forall x, y)$ $x \equiv y \pmod{n}$

$\iff x \equiv y \pmod{p}$ & $x \equiv y \pmod{q}$

Proof: $$e \cdot d = 1 \pmod{\phi(n)}$$
$$= 1 + t \cdot (p-1) \cdot (q-1)$$
$$= 1 \pmod{(p-1)} = 1 + u(p-1)$$

Want to show $(\forall m)$ $m^{ed} = m \pmod{p}$

Case 1: $m = 0 \pmod{p}$ ✓

Case 2: $m \neq 0 \pmod{p} \iff m \in \mathbb{Z}_p^*$

$\implies m^{p-1} \equiv 1 \pmod{p}$ Fermat Little theorem

$$m^{ed} = m^{1+u(p-1)}$$
$$= m \cdot (m^{p-1})^u \pmod{p}$$
$$= m \cdot 1 \equiv m$$

$\therefore$ $m^{ed} = m \pmod{p}$ for all m

Similarly $m^{ed} = m \pmod{q}$ for all m

By CRT, $m^{ed} = m \pmod{n}$ for all m

$\forall m \in \mathbb{Z}_n$ $D(E(m)) = m$ $\boxtimes$