Admin:

Outline: PK encryption

- ☐ El Gamal encryption (review)
- ☐ Semantic security def
- ☐ Thm: El Gamal is semantically secure
- ☐ IND-CCA2 (ACCA) security
- ☐ Cramer-Shoup PK encryption
- ☐ RSA

El Gamal encryption (Taher El Gamal, 1984)

- Public key encryption scheme
  - Keygen$(1^\lambda) \longrightarrow (PK, SK)$ λ = "security parameter"
  - $E(PK, m) \longrightarrow c$ [may be randomized $E(PK, m, r)$
  - $D(SK, c) \longrightarrow m$ deterministic

- Let $G = \langle g \rangle$ be a cyclic group
- We suppose $m \in G$, via suitable encoding

- **Keygen:** pick $SK = x$ $0 \le x < |G|$
  let $PK = g^x$ } Alice's PK

- **Encryption:** (randomized) let $PK = y$ of recipient ($y = g^x$, Alice)
  pick k at random $0 \le k < |G|$
  let $c = (g^k, m \cdot y^k)$ ciphertext

- **Decryption:** let $c = (a, b)$ received ciphertext
  then $m = b / a^x$ $(SK = x)$
  [Note: $a^x = g^{kx} = y^k$]

- Relation to DH key exchange

Alice $\xrightarrow{\quad y = g^x \text{ (via PKI?)} \quad}$ Bob

$\xleftarrow{\quad a = g^k \quad}$

$\xleftarrow{\quad b = m \cdot \text{key} \quad}$

DH key $= (g^k)^x = g^{xk} = a^x$

DH key $= (g^x)^k = y^k = g^{xk}$

Semantic Security

- early def of security for PK enc (Goldwasser/Micali)
- Adversary can't tell $E(m_0)$ from $E(m_1)$
- Game

Keygen $\to$ (PK, SK) $\xrightarrow{\quad PK \quad}$ Adv

$\xleftarrow[m_0 \neq m_1]{m_0,\ m_1}$

pick $b \in_R \{0,1\}$ $\xrightarrow{\quad E(m_b) \quad}$

$\xleftarrow{\quad \hat{b} \quad}$

$\underbrace{b \stackrel{?}{=} \hat{b}}$

if yes, adversary wins.

- Scheme is <u>semantically</u> <u>secure</u> if $\Pr[\text{Adv wins}] \le \frac{1}{2} + \text{negligible}$
- (Note: scheme <u>must be</u> <u>randomized</u> to be sem. secure, at least...)
- Is El Gamal semantically secure?
- Recall DDH:

  distinguishing (g^a, g^b, g^c) from (g^a, g^b, g^{ab}) is hard.

  a, b, c random $\qquad\qquad$ a, b random

  [Note: Boneh presented this as

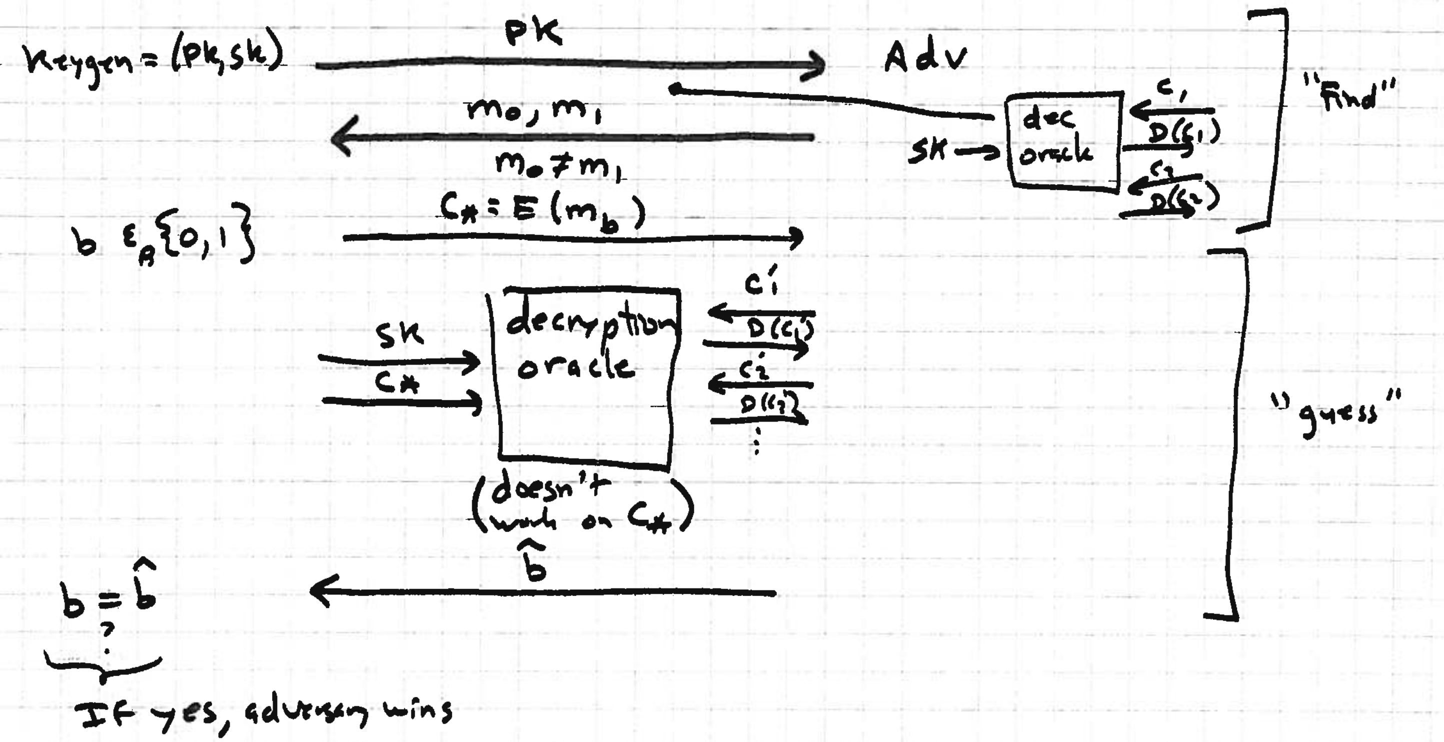
  four tuple (g, g^a, h, h^d) is $a \stackrel{?}{=} d$

  is the same (g, g^a, g^b, g^{bd}) is $a \stackrel{?}{=} d$

- <u>Theorem</u> (Tsiounis & Yung):

  El Gamal is sem secure $\iff$ DDH holds in G

- Sem. security may not be enough:
  - El Gamal is <u>malleable</u>: Given $E(m) = (g^k, m \cdot y^k)$
    easy to produce $E(2m) = (g^k, 2 \cdot m \cdot y^k)$
    without knowing m!
    (Imagine I want to outbid you at an auction.
  - Also, not IND-CCA2 secure (ACCA) adaptive chosen-ciphertext attack



- Scheme is ACCA secure (IND-CCA2 secure) if
  Prob(Adv wins) $\leq \frac{1}{2}$ + negligible

- El Gamal is not IND-CCA2 secure:
  Given $c_* = (g^k, m \cdot y^k)$
  ask to decrypt $c_*' = (g^k, 2my^k) \Rightarrow 2m \stackrel{\div 2}{\Rightarrow} m$

- El Gamal is <u>homomorphic</u>: $c_1 \in E(m_1) = (g^r, m_1 \cdot y^r)$
  $c_2 \in E(m_2) = (g^s, m_2 \cdot y^s)$

  $c \cdot c_1 \quad = (g^{r+s}, m_1 \cdot m_2 \cdot y^{r+s}) = E(m_1 \cdot m_2)$

6.857 Rivest
3/16/09 L12.5

Cramer-Shoup

IND-CCA2 secure
Can be viewed as elaboration of El Gamal
One of simpler ones. "Plaintext aware"...

Let G_q be group of prime order q (E.g. squares in Z_p^*, where $p=2q+1$).

Keygen:

$g_1, g_2 \in_R G_q$

$x_1, x_2, y_1, y_2, z \in_R Z_q$

H: hash fn mapping $G_q^3 \to Z_q$

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

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

$h = g_1^z$ ← EG

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

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

Encrypt (m): $(m \in G_q)$

$r \in_R Z_q$ ← EG

$u_1 = g_1^r$

$u_2 = g_2^r$

$e = h^r \cdot m$ ← EG

$\alpha = H(u_1, u_2, e)$

$v = c^r d^{r\alpha}$

ciphertext $= (u_1, u_2, e, v)$

Decrypt (u_1, u_2, e, v):

$$\alpha = H(u_1, u_2, e)$$

check: $u_1^{x_1+y_1\alpha}\, u_2^{x_2+y_2\alpha} \stackrel{?}{=} v$

if not =, reject

output: $m = e/u_1^z$ ← EG

Note: $u_1^{x_1} u_2^{x_2} = g_1^{rx_1} g_2^{rx_2} = c^r$

$u_1^{y_1} u_2^{y_2} = d^r$

$u_1^z = g_1^{rz} = h^r$

Thm: Cramer Shoup is secure against adaptive chosen ciphertext attack (IND-CCA2 secure) if DDH assumption holds in G_q and H satisfies a certain condition (≈"target collision resistance").

Thus, this strongest notion of security for PK encryption is achievable, albeit at some cost in terms of speed & complexity.

RSA encryption

Keygen: p, q random primes (e.g. 512-bit)

$n = p \cdot q$

$e \in_R Z^*_{\varphi(n)}$ $\quad (\varphi(n) = (p-1)\cdot(q-1)$; $\gcd(e, \varphi(n)) = 1)$

$d = e^{-1} \pmod{\varphi(n)}$

[e can be short; d shouldn't be]

$PK = (n, e)$

$SK = (d, p, q)$

Factoring: Assume it is infeasible for an adversary to produce p & q, given n, where p, q randomly chosen.

($\approx$ DLP for El Gamal) [RSA-200 (663 bits) factored 2005 NFS]

Enc: Given $m \in Z_n$ & $PK = (n, e)$:

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

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

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

~~Fact: $(\forall m \in Z_n)$ $m^{k\cdot\varphi(n)+1} \equiv m$ $(\forall k)$ (mod n)~~

~~[Prove mod p & mod q, then use CRT] [Easy if $m \in Z_n^*$]~~

~~$(\forall m \in Z_n)$ $D(E(m)) = m$~~

Correctness of RSA:

Lemma: (Chinese remainder theorem or CRT)

Let $n = p \cdot q$ $\quad p, q$ distinct primes

Then $(\forall x, y)$ $\quad x \equiv y \pmod n \iff x \equiv y \pmod p \;\&\; x \equiv y \pmod q$

So: **Prove RSA correct mod p:** (similarly mod q)

$$e \cdot d = 1 \pmod{\varphi(n)}$$

$$e \cdot d = 1 + t \cdot (p-1) \cdot (q-1)$$

$$e \cdot d = 1 \pmod{(p-1)}$$

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

Case 1: $\quad m = 0 \pmod p$ ✓

case 2: $\quad m \neq 0 \pmod p$

$$\iff m \in Z_p^*$$

$$\Rightarrow m^{p-1} \equiv 1 \pmod p$$

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

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

$$\equiv m \cdot 1$$

$$\equiv m$$

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

$\therefore\ m^{ed} = m \pmod q$ " " "

$\therefore\ m^{ed} = m \pmod n$ " " "

$$(\forall m \in Z_n)\ D(E(m)) = m$$