6.857 Rivest
3/9/11 L11.1

Admin: PS #3 posted today

Outline: PKE – public key encryption

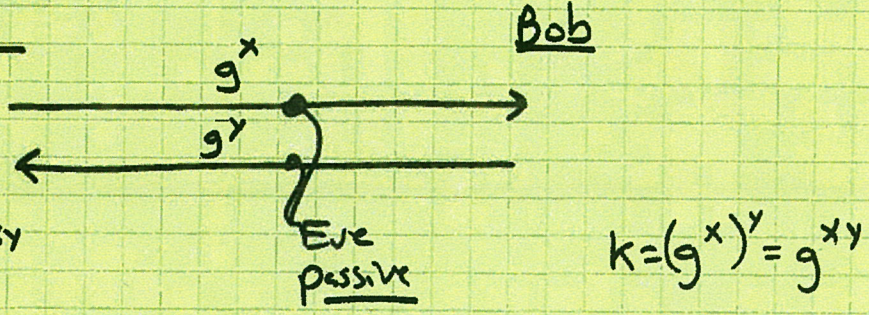
- DH key exchange review
- CDH & DDH
- RSA
- El Gamal
- Semantic security
- IND-CCA2
- Cramer-Shoup

Diffie Hellman key exchange

p, g public parameters

Alice: secret key x, public key g^x (permanent or transient)

Bob: secret key y, public key g^y (" " ")



requires DLP to be hard, but not known to be sufficient

CDH: given g^x & g^y, to compute g^{xy} (is hard)
(Computational Diffie Hellman assumption.)

CDH ⇒ DH key exchange is secure (against passive eavesdropper) (Duh!)
(for secrecy key)

Related problem:

DDH: Given (g^a, g^b, g^c) a, b, c random
or (g^a, g^b, g^{ab}) a, b random

— to be able to distinguish the two cases... (is hard)
"Decision diffie hellman"

DDH ⇒ CDH (i.e. ¬CDH ⇒ ¬DDH)

Is DDH easier than CDH??
in some groups???
recognizing right answer g^{ab} might be
easier than computing it...??

RSA encryption

3/9/11 L11.3

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

$n = p \cdot q$

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

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

[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 bit) factored 2005 NFS]

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

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

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

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

[illegible]

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: $m = 0 \pmod{p}$ ✓

Case 2: $m \neq 0 \pmod{p}$

$\Leftrightarrow m \in \mathbb{Z}_p^*$

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

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

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

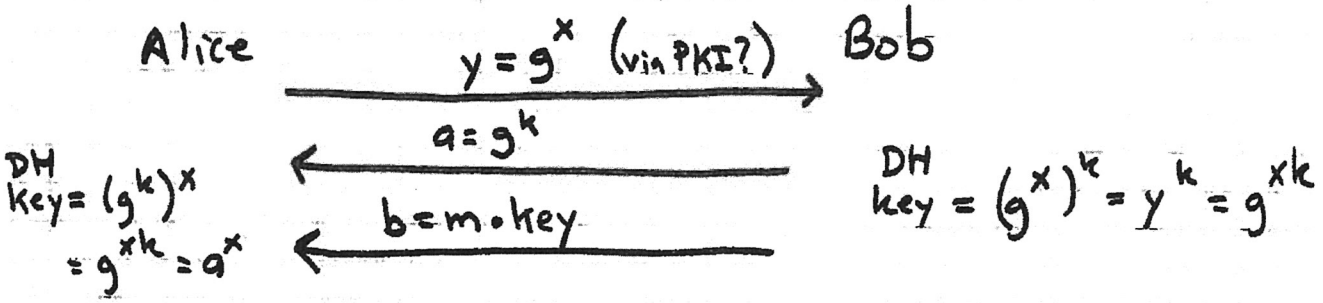
$\therefore m^{ed} = m \pmod{q}$ " " "

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

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

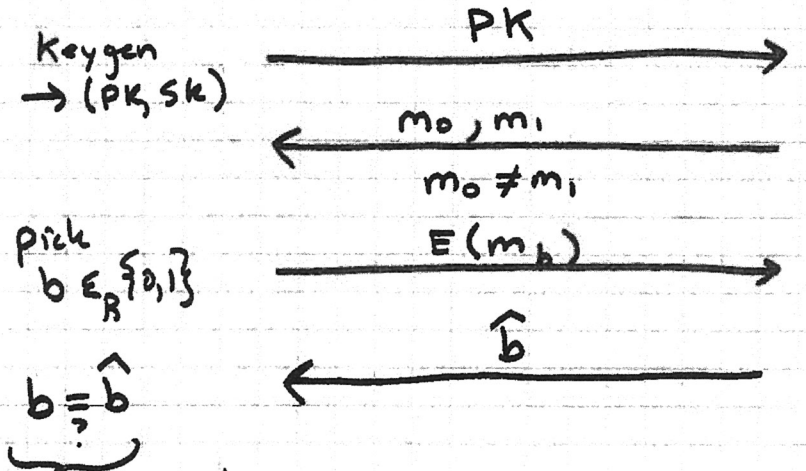
ElGamal encryption (Taher ElGamal, 1984)

- 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 $SK = x$ $0 \le x < |G|$ } Alice's PK
  let $PK = g^x$
- Encryption: (randomized) let $PK = y$ of recipient Alice $(y = g^x)$
  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



Semantic Security

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



- Scheme is semantically secure if $Pr[\text{Adv wins}] \leq \frac{1}{2} + \text{negligible}$
- (Note: scheme must be randomized 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 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 $a \stackrel{?}{=} d$

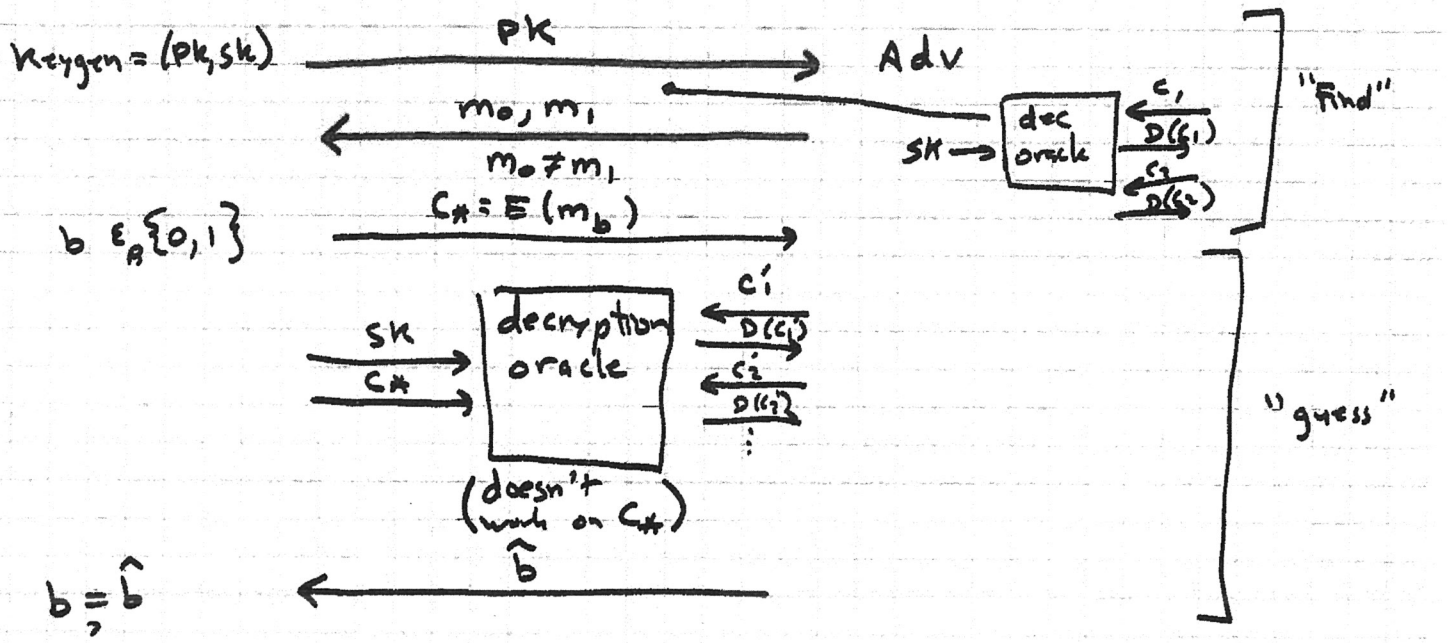
- **Theorem** (Tsiounis & Yung):

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

- Sem. security may not be enough:
  - El Gamal is malleible: 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 $C^{*\prime} = (g^k, 2m y^k) \Rightarrow 2m \xrightarrow{\div 2} m$

- El Gamal is homomorphic: $C_1 \in E(m_1) = (g^r, m_1 \cdot y^r)$
  $C_2 \in E(m_2) = (g^s, m_2 \cdot y^s)$
  $C \cdot C_1 = (g^{r+s}, m_1 \cdot m_2 \cdot y^{r+s}) = E(m_1 \cdot m_2$

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

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

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

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.