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 $p$

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

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

**Encryption**

Bob does the following

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

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

(c) $y = g^k \mod p, \quad s = m \cdot (g^x)^k \mod p$

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

**Decryption**

To recover plaintext, Alice does

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

(b) Recover $m = (y^{-x}) \cdot s \mod p$

$g^{-kx} \cdot m \cdot g^{kx}$
Semantic Security

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

\[
\text{Keygen}(PK, SK) \quad \rightarrow \quad PK \quad \rightarrow \quad \text{Adv}
\]

\[
\begin{align*}
\text{pick } b & \in \{0, 1\}^* \\
b & = \hat{b} \quad ?
\end{align*}
\]

If yes, adversary wins

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

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 $a, b$ random

Theorem (Tsiounis & Yung):
El Gamal is semantically secure $\Leftrightarrow$ DDH holds in $G$
El Gamal is malleable

Given $E(m) = (g^k, m \cdot g^{xk})$

Easy to produce $E(2m) = (g^k, 2m \cdot g^{xk})$

Without knowing $m$! (Can outbid you at an auction)

IND-CCA2: Adaptive chosen ciphertext attacks

non-adaptive: IND-CCA1

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

$SK \rightarrow$ Decryption Oracle

$C_x = E(m_b) \\ b \in_R \{0, 1\} \\ c_x \rightarrow D(c_1) \\ c_2 \rightarrow D(c_2)$

$b = b$?

If yes, adversary wins

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

El Gamal is not IND-CCA2 secure

Given $C_x = (g^k, m \cdot g^{xk})$ ask to decrypt

$C_x = (g^k, 2mg^{xk}) \Rightarrow 2m \Rightarrow m$ known

Homo morphic: $E(m_1) \cdot E(m_2) = E(m_1m_2)$
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 $G$

$x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$ \{0, 1, ..., $q-1$\}

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

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

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
\[
\begin{align*}
n &= p \cdot q \\
\phi(n) &= (p-1)(q-1) \\
\end{align*}
\]
\( e \in \mathbb{Z}_n^* \), \( \phi(n) \) need \( \text{gcd}(e, \phi(n)) = 1 \)
\[
d = e^{-1} \pmod{\phi(n)} \quad \{ \text{e can be short;} \}
\]
\[
\text{d shouldn't be}\] 
\[\text{use Extended Euclidean algorithm}\]
\[
PK = (n, e) \\
SK = (d, p, q)
\]

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 \( c \) & \( SK = (d, p, q) \)
\[
m = D(c) = cd \pmod{n}
\]

\( p \) & \( q \) 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 \((\forall x, y) \quad x \equiv y \pmod{n} \) 
\[
\iff x \equiv y \pmod{p} \quad \& \quad x \equiv y \pmod{q}
\]

**Proof:** \[e,d = 1 \pmod{\phi(n)}\]
\[= 1 + \tau(p-1)(q-1)\]
\[= 1 \pmod{(p-1)} = 1 + u(p-1)\]

Want to show \((\forall m) \quad m^{ed} \equiv m \pmod{p}\)

**Case 1:** \( m = 0 \pmod{p} \)

**Case 2:** \( m \neq 0 \pmod{p} \)  \(\equiv m \in \mathbb{Z}_p^*\)

\[
\Rightarrow m^{p-1} \equiv 1 \pmod{p}
\]

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

\[\forall \quad m^{ed} = m \pmod{p} \quad \text{for all } m
\]

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

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

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