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^k) → (PK, SK)
  - E(PK, m) → c
  - D(SK, c) → m
deterministic

- Let G=<g> be a cyclic group
- We suppose m ∈ G, via suitable encoding

  - Keygen: pick SK=x, 0 ≤ x < |G| → Alice’s PK let PK=g^x

  - Encryption: (randomized) let PK=y, PK received ciphertext (y=g^x, Alice)
      pick k at random 0 ≤ k < |G|
      let c=(g^k, m•y^k)

  - 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       y=g^x (via PK?) → Bob
              \[ a=g^k \]
              \[ b=m•key \]

  DH key = (g^k)^x = g^{kx} = 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

\[
\text{Keygen} \rightarrow (PK, SK) \quad \xrightarrow{\text{PK}} \quad \text{Adv} \\
\xleftarrow{\text{mo, mi}} \\
\xleftarrow{\text{mo \neq mi}} \\
pick \quad b \in \{0, 1\} \\
\xrightarrow{\text{E(m_b)}} \\
\xleftarrow{\hat{b}} \\
\text{if yes, adversary wins.}
\]

- Scheme is semantically secure if \( \Pr[\text{Adv wins}] \leq \frac{1}{2^n} + \text{negligible} \)
  (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
- \(a\) and \(b\) random

[Note: Boneh presented this as
- four tuple \((g, g^a, h, h^d)\) is \(a = d\)
- the same \((g, g^a, g^b, g^{bd})\) is \(a = d\)

Theorem (Tsiounis & Yung):

- El Gamal is sem secure \(\iff\) DDH holds in \(G\)
- Sem. security may not be enough:
  - El Gamal is malleable: \[
  \frac{\text{Given } E(m) = (g^k, m \cdot y^k)}{\text{can to produce } E(2m) = (g^k, 2 \cdot m \cdot y^k)}
  \]
  without knowing \( m \)?
  (Imagine I want to outbid you at an auction.)

- Also, not IND-CCA2 secure (ACCA) adaptive chosen-ciphertext attack

\[
\begin{align*}
\text{Keygen} = (pk, sk) & \quad \xrightarrow{\text{PK}} \quad \text{Adv} \\
\text{b \in \{0, 1\}} & \xrightarrow{\text{0 or 1}} \quad \text{dec oracle} \\
\text{sk} \xrightarrow{\text{sk}} & \quad \text{enc oracle} \\
\text{C_a = E(m)} & \xrightarrow{\text{C_a}} \quad \text{dec oracle} \\
\text{(doesn't \'t work on C_a)} & \xrightarrow{\text{yes or no}} \quad \text{"guess"} \\
\text{b = b} & \xrightarrow{\text{yes or no}} \quad \text{Adv wins}
\end{align*}
\]

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

- El Gamal is not IND-CCA2 secure:
  \[
  \begin{align*}
  \text{Given } C = (g^k, m \cdot y^k) & \quad \text{can to decrypt } C' = (g^k, 2m \cdot y^k) = 2m \not\equiv m \\
  \text{El Gamal is homomorphic: } & \quad C_1 \cdot E(m_1) = (g^{r_1}, m_1 \cdot y_1^r) \\
  & \quad C_2 \cdot E(m_2) = (g^{r_2}, m_2 \cdot y_2^r) \\
  \end{align*}
  \]
  \[
  \quad \quad c \cdot c_1 = (g^{r + 5}, m_1 \cdot m_2 \cdot y_1^r \cdot y_2^r) = E(m_1 \cdot m_2)
  \]
Cramer-Shoup

IND-CCA2 secure
Can be viewed as elaboration of El Gamal
One of simpler ones, “Plaintext sworn” ...

Let $G_q$ be group of prime order $q$ (e.g., squares in $\mathbb{Z}_p^*$, where $p=2q+1$).

Keygen:
\[ g_1, g_2 \in_R G_q \]
\[ x_1, x_2, y_1, y_2, z \in_R \mathbb{Z}_q \]
\[ H: \text{hash fn mapping } G_q^3 \to \mathbb{Z}_q \]
\[ c = g_1^{x_1} g_2^{x_2} \]
\[ d = g_1^{y_1} g_2^{y_2} \]
\[ h = g_1^z \]
\[ PK = (g_1, g_2, c, d, h, H) \]
\[ SK = (x_1, x_2, y_1, y_2, z) \]

Encrypt $(m)$:
\[ (m \in G_q) \]
\[ r \in_R \mathbb{Z}_q \]
\[ u_1 = g_1^r \]
\[ u_2 = g_2^r \]
\[ e = h^r \cdot m \]
\[ \alpha = H(u_1, u_2, e) \]
\[ v = c^r d^r \alpha \]
\[ \text{ciphertext} = (u_1, u_2, e, v) \]
Decrypt \((u_1, u_2, e, v)\):

\[\alpha = H(u_1, u_2, e)\]

check: \[u_1^{x_1 + y_1 \alpha} u_2^{x_2 + y_2 \alpha} \equiv v\]

if not, \textbf{reject}

output: \[m = e / u_1^{\alpha}\]

\[m = e / u_1^{\alpha}\]

\[v = e / u_1^{\alpha}\]

\[v = e / u_1^{\alpha}\]

\[v = e / u_1^{\alpha}\]

\[v = e / u_1^{\alpha}\]

Note: \[u_1^{x_1} u_2^{x_2} = g_1^{r_{x_1}} g_2^{r_{x_2}} = c^r\]

\[u_1^{y_1} u_2^{y_2} = d^r\]

\[u_1^{\alpha} = g, u_1^{\alpha} = h^r\]

Thm: Cramer–Shoup is secure against adaptive chosen ciphertext attack (IND-CCA2 secure) if DDH assumption holds in \(G_8\) and \(H\) satisfies a certain condition (\(\approx\) "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:**

\[
p, q \text{ random primes (e.g. 512-bit)}
\]

\[
n = p \cdot q
\]

\[
e \in \mathbb{Z}_n^* \quad (\varphi(n) = (p-1)(q-1) \wedge \text{gcd}(e, \varphi(n)) = 1)
\]

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

\[\text{[e can be short; } d \text{ shouldn't be]}\]

\[
PK = (n, e)
\]

\[
SK = (d, p, q)
\]

**Factoring:** Assume it is infeasible for an adversary to produce \(p \cdot q\), given \(n\), where \(p, q\) randomly chosen.

\[\approx \text{DLP for El Gamal} \quad [\text{RSA-200 (663 bit) factored 2005 NFS}]\]

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

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

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

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

\[\text{[exponentiation of } c\text{]}\]

\[\text{[large numbers, public-key cryptography]}\]

\[c \cdot d \equiv 1 \pmod{\varphi(n)}\]
Correctness of RSA:

Lemma: (Chinese remainder theorem or CRT)
Let \( n = p \cdot q \) be 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 \( \mod{p} \); (similar \( \mod{q} \))
\[
e \cdot d = 1 \pmod{\phi(n)}
\]
\[
e \cdot d = 1 + t \cdot (p-1) \cdot (q-1)
\]
\[
e \cdot d = 1 \pmod{(p-1)}
\]

We want to show \( (\forall m) \quad m^{ed} = m \pmod{p} \)

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

**Case 2:** \( m \neq 0 \pmod{p} \)
\[\iff m \in \mathbb{Z}_p^* \]
\[\Rightarrow m^{p-1} \equiv 1 \pmod{p} \]
\[m^{ed} \equiv m^{1 + t \cdot (p-1)} \equiv m \cdot (m^{p-1})^t \pmod{p} \]
\[\equiv m \cdot 1 \equiv m \]
\[\therefore m^{ed} = m \pmod{p} \quad \text{for all } m \]
\[\therefore m^{ed} = m \pmod{q} \quad \therefore \]
\[\therefore m^{ed} = m \pmod{n} \quad \therefore \]

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