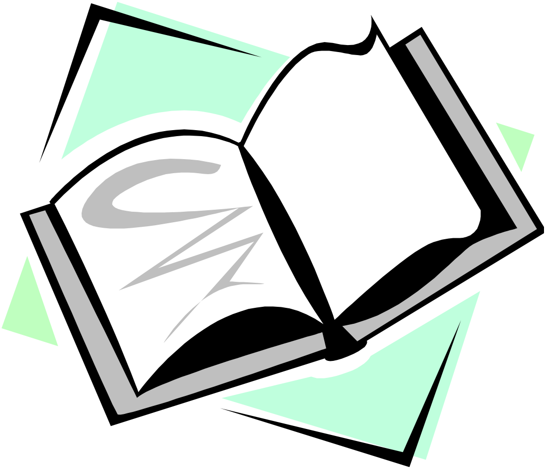
Cryptography
CS 555

Topic 19: Formalization of Public Key Encrpytion

Outline and Readings

- Outline
  - CPA Security for public key encryption
  - Hybrid encryption
  - Padded RSA
  - El Gamal Encryption
  - CCA Security for public key encryption



- Readings:
  - Katz and Lindell: Section 10.2, 10.3, 10.4, 10.5, 10.6

IND-CPA Security

- For public key encryption, Ciphertext Indistinguishability against Chosen Plaintext Attacker is equivalent to Ciphertext Indistinguishability against Eavesdroppers
  - Because one gets the Encryption Oracle for free in public key encryption schemes

Hybrid Encryption

- Construction 10.12. Given a CPA-secure public-key encryption Enc_{pk}, and a private key encryption scheme E_k.
  - To encrypt a message *m*, randomly choose $k \leftarrow \{0,1\}^n$,
  - Cipheretext is $\langle Enc_{pk}(k), E_k(m) \rangle$
  - A new *k* is chosen for each encryption; encryption is randomized

Hybrid Encryption is Secure

- Theorem 10.13: If Enc_{pk} is CPA-secure, and E_k is secure against eavesdropper, then Construction 10.12 is CPA-secure.
  - Why E_k only needs to be secure against eavesdropper, and does not need to be CPA-secure?
- Proof idea. Need to show the following are IND

  $a=\langle pk, \text{Enc}_{pk}(k), E_k(m_0)\rangle$ $\quad$ $d=\langle pk, \text{Enc}_{pk}(k), E_k(m_1)\rangle$
- Consider

  $b=\langle pk, \text{Enc}_{pk}(0^n), E_k(m_0)\rangle$ $\quad$ $c=\langle pk, \text{Enc}_{pk}(0^n), E_k(m_1)\rangle$
- (a,b), (c,d) IND because Enc_{pk} is secure; (b,c) IND because E_k is secure.
- This proof technique is known as Hybrid argument.

Simply Padded RSA

- Construction 10.18. To encrypt *m* using RSA, randomly chooses *r* (so that *r*||*m* is of length ||N||-1), compute ciphertext $c := [(r||m)^e \bmod N]$
- When m is really short (O(log ||N||)), this construction can be prove secure assume that the RSA problem is hard.
  - That is, computing O(log ||N||) least significant bits of the e’th root is as hard as computing the e’th root
  - When r is not that long, there exists no proof of the security of the construction under the assumption that the RSA problem is hard.

RSA-OAEP

- Optimal Asymmetric Encryption Padding (OAEP)
  - Roughly, to encrypt m, chooses random r, encode m as $m' = [X = m \oplus H_1(r)\ ,\ Y = r \oplus H_2(X)\ ]$ where H_1 and H_2 are cryptographic hash functions, then encrypt it as $(m')^e \bmod n$
  - To decrypt $m'=[X,Y]$, compute $r = Y \oplus H_2(X)$, and $m = X \oplus H_1(r)$

- Proven secure under the RSA assumption when H_1 and H_2 are assumed to be random oracles.
  - Unless both X and Y are fully recovered, cannot obtain r, without r, cannot obtain any information of m.
  - We will not cover Random Oracle Model in this course. See Chapter 13 if interested.

ElGamal Encryption

- Public key <p, g, $h=g^a$ mod p>
- Private key is a
- To encrypt m: chooses random b, computes
  $C=[g^b \bmod p,\ h^b m \bmod p]$.
  - Idea: for each m, sender and receiver establish a shared secret $h^b = g^{ab}$ via the DH protocol. The value g^{ab} hides the message m by multiplying it.
- To decrypt $C=[c_1,c_2]$, computes $[c_2 / (c_1^a \bmod p) \bmod p]$.

El Gamal Encryption is CPA-secure under DDH Assumption

- Decision Diffie Hellman (DDH) Problem: Given (g,g^x,g^y,g^z) sampled either from (g, g^a,g^b,g^{ab}) or from (g, g^a,g^b,g^c), tell which is the case
  - a,b,c uniformly randomly chosen from [1,p-1]
- Given adversary A for El Gamal encryption, construct adversary for DDH problem as follows:
  - Take (g,g^x,g^y,g^z) as input, use (g, g^y) as public key, when A outputs (m_0,m_1), encrypt m_b as $(g^x, g^z m_b)$ and send to A. If A wins, outputs sampled from (g, g^a,g^b,g^{ab})
  - When (g,g^x,g^y,g^z) sampled from (g, g^a,g^b,g^c), $g^z m_b$ has uniform distribution and independent from g^x,g^y

Chosen Ciphertext Security

- Most public key encryption schemes we have examined are insecure against chosen ciphertext attacks
  - Textbook RSA: Given a RSA ciphertext $c=m^e \bmod N$, construct $c'=c2^e \bmod n$, after obtaining plaintext m', compute $m' \cdot 2^{-1} \bmod n$
  - El Gamal: Given $C=[g^b \bmod p, h^b m \bmod p]$, how to change the ciphertext?
  - What about Simply Padded RSA: $c=(r||m)^e \bmod N$?
    - Insecure.
  - What about RSA-OAEP?
    - Secure, why?

Coming Attractions …

- Other Public Key Encryption Schemes

- Reading: Katz & Lindell: Chapter 11