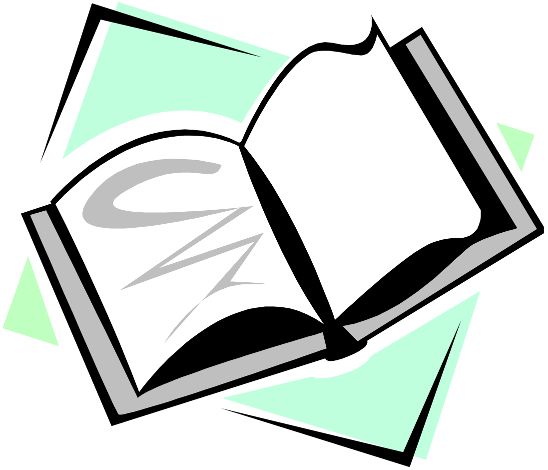
Cryptography
CS 555

Topic 7: Stream Ciphers and CPA Security

Outline and Readings

- Outline
  - Handling variable length messages
  - Security for multiple messages
  - Stream ciphers for multiple messages
  - CPA secure



- Readings:
  - Katz and Lindell: 3.4, 3.5

Handling Variable Length Messages (Textbook, Section 3.4.2)

- A variable output-length pseudo-random generator is $G(s, 1^{\ell})$ that output ℓ such that
  - Any shorter output is the prefix of the longer one
  - Fix any length, this is a pseudo-random generator

- Given such a generator, can encrypt messages of different length by choosing ℓ to be length of the message.

Security for Multiple Encryptions (Textbook Section 3.4.3)

- How to encrypt multiple messages with one key?
  - What is wrong with using the standard way of using stream cipher to encrypt?

- How to define secure encryption with multiple messages?

Definition 3.18. Has indistinguishable Multiple Encryptions in the presence of an eavesdropper.

- Define an experiment called $\mathbf{PrivK^{mult}}(n)$
  - Involving an Adversary and a Challenger
  - Instantiated with an Adv algorithm $\mathcal{A}$, and an encryption scheme Π = (Gen, Enc, Dec)

Challenger

$k \leftarrow Gen(1^n)$

$b \leftarrow_R \{0,1\}$

Adversary

$\mathcal{A}(1^n)$ gives two vector of messages such that corresponding msgs have equal lengths

Adversary → Challenger: M_0, M_1

Challenger → Adversary: $C=\mathbf{E}_k[m_b^1], \mathbf{E}_k[m_b^2], \ldots \mathbf{E}_k[m_b^t]$

Adversary → Challenger: $b' \in \{0,1\}$

$\mathbf{PrivK^{mult} = 1}$ **if b=b', and** $\mathbf{PrivK^{mult} = 0}$ **if** $\mathbf{b \neq b'}$

$\Pr[\mathbf{PrivK^{mult}}_{\mathbf{A,\Pi}}=1] \leq ½ + negl(n)$

Single Msg vs. Multiple Msgs

- Give an encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper
  – i.e., secure in single message setting
- But does not have indistinguishable multiple encryptions in the presence of an eavesdropper.
  – i.e., insecure for encrypting multiple messages?

- No deterministic encryption scheme is secure for multiple messages

How to Encrypt Multiple Messages with a Stream Cipher (i.e., Pseudorandom generator)

- Method 1: Synchronized mode
  - Use a different part of the output stream to encrypt each new message
  - Sender and receiver needs to know which position is used to encrypt each message
  - Often problematic

How to Encrypt Multiple Messages with a Stream Cipher

- Method 2: Unsynchronized mode
  - Use a random Initial Vector (IV)
  - $\mathbf{Enc}_k(m) = \langle IV, G(k,IV) \oplus m \rangle$
    - IV must be randomly chosen, and freshly chosen for each message
    - How to decrypt?
  - What G to use and under what assumptions on G such a scheme has indistinguishable multiple encryptions in the presence of an eavesdropper
    - What if $G(k,IV) \equiv G'(k||IV)$, where G' is a pseudorandom generator

Security of Unsynchronized Mode

- Recall that
  - IV is sent in clear, so is known by the adversary
  - For each IV, G(·,IV) is assumed to be pseudorandom generator;
  - Furthermore, when given multiple IVs and outputs under the same randomly chosen seed, the combined output must be pseudo-random
  - Stream ciphers in practice are assumed to have the above **augmented pseudorandomness** property and used this way

Functions and Keyed Functions

- Consider $\mathbf{Enc}_k(m) = \langle IV, G(k,IV) \oplus m \rangle$
- $G(k,IV)$ takes two inputs. This can also be viewed as a family (set) of functions, aka, a keyed function
- For each key k, we define function G_k to be $G_k(x) = G(k,x)$
- The property we desire for G is such that when k is randomly chosen, $G_k(\cdot)$ has the property that knowing $G_k(x_1)$ one cannot predict what will $G_k(x_2)$ be $x_1 \neq x_2$
  – That is, $G_k(\cdot)$ should be indistinguishable from a random function.
  – If one can predict $G_k(x)$ when given x, is the above encryption scheme secure?

Security Against Chosen Plaintext Attacks (Textbook 3.5)

- Security notions considered so far is for ciphertext-only attacks
- Modeling chosen plaintext attacks
  - Adversary may choose messages and obtain corresponding ciphertexts adaptively
    - Adaptively means that adversary may look at the ciphertext of the first chosen message, then choose the next message.
  - How to model this ability of the adversary?
    - Adversary is given an **encryption oracle**, which can encrypt messages but does not give out the key

The CPA Indistinguishablility Experiment: **PrivK^{cpa}**(n)

- A k is generated by Gen(1^n)
- Adversary is given oracle access to $Enc_k(\cdot)$, and outputs a pair of equal-length messages m_0 and m_1
- A random bit b is chosen, and adversary is given $Enc_k(m_b)$
  - Called the challenge ciphertext
- Adversary still has oracle access to $Enc_k(\cdot)$, and (after some time) outputs b'
- **PrivK^{cpa}**(n) = 1 if b=b' (adversary wins) and =0 otherwise

CPA-secure (aka IND-CPA security)

- A private-key encryption scheme Π = (Gen, Enc, Dec) has indistinguishable encryption under a chosen-plaintext attack iff. for all PPT adversary *A*, there exists a negligible function negl such that
  - $\Pr[\mathbf{PrivK}^{\mathbf{cpa}}_{A,\Pi}=1] \leq \frac{1}{2} + \mathrm{negl}(n)$
- No deterministic encryption scheme is CPA-secure. Why?

Properties of CPA-secure

- CPA-secure for multiple messages is equivalent to CPA-secure for a single message

- Given a fixed-length encryption scheme that is CPA-secure, we can encrypt messages of arbitrary length by encrypting different parts of messages separately

Coming Attractions …

- Pseudorandom functions
- Reading: Katz & Lindell: 3.6