Cryptography
CS 555

Topic 21: Midterm Review

Course Business

- Midterm is on Wednesday (in class)
    - Allowed to bring one index card (double sided)
    - 3x5 inches
    - Good review, but you won’t have time to consult for every question
- Format: Multiple Choice/True-False/Select all that Apply
- Everything we have covered in lecture is fair game for midterm

Good Things to Know

- Perfect Secrecy
  - Definition(s)/Constructions/Limitations/Required Properties
- Security against Eavesdropping Attacks
  - Single Eavesdropping
  - Multiple Eavesdropping
  - Constructions
  - Limitations

Good Things to Know

- Chosen Plaintext Attacks and CPA-Security
    - Definition
    - Constructions
    - Showing a scheme is not CPA-secure
    - Required Properties

- CCA-Secure Encryption
    - Definition
    - Constructions
    - Showing a scheme is/is not CPA-secure
- Authenticated Encryption

Good Things to Know: Primitives

- PRGs
  - Definition
  - And how to use them
  - Example: Construct encryption scheme with security against eavesdropping attacks
    - Correction: $\mathrm{Enc}_{\mathrm{K}}(\mathrm{m}) = \mathrm{G}(m) \oplus m$
    - Secure against single eavesdropping attacks, but not multiple
- PRFs and PRPs (pseudorandom permutation)
  - Security Definitions
  - And how to use them
  - Examples:
    - Construct MACs (bounded length)
    - Construct CPA-Secure Encryption

Good Things to Know

- MACs
    - Secrecy vs Integrity
    - Security Definition
    - Constructions
        - Fixed Length: $MAC_K(m) = f_K(m)$
- Collision Resistant Hash Functions
    - Definition
    - Applications
    - Generic Attacks
    - Random Oracle Model

Block Ciphers

- Substitution Permutation Network
  - AES
  - S-boxes
  - How to encrypt/decrypt
- Feistel Network
  - DES/3DES
  - S-boxes
  - How to encrypt/decrypt

Good Things to Know

- One-way functions
  - Definition
  - Necessary for Private Key Crypto
  - Sufficient for Private Key Crypto
  - Does it hide information about input?
- Hard Core Predicates
  - Definition
  - Application(s)

- These two topics will be tested less heavily

Example Question

Let F_K be a PRF with n-bit inputs/outputs and let

$$MAC_K(m_1, \dots, m_8) = F_K(m_1) \| F_K(m_2) \| \dots \| F_K(m_8)$$

True (T) or False (F) or More Information (M): The above construction is a secure MAC for messages of length 8n.

Example Question

Let F_K be a PRF with n-bit inputs/outputs and let

$$MAC_K(m_1, \ldots, m_8) = F_{K_1}(m_1) \| F_{K_2}(m_2) \| \ldots \| F_{K_8}(m_8)$$

True (T) or False (F) or More Information (M): The above construction is a secure MAC for messages of length 8n.

Example Question

Let F_K be a PRF with n-bit inputs/outputs and let

$$MAC_K(m_1, \dots, m_8) = F_{K_1}(000\|m_1)\big\|F_{K_2}(001\|m_2)\big\|\dots\|F_{K_8}(111\|m_8)$$

True (T) or False (F) or More Information (M): The above construction is a secure MAC for messages of length 8n.

Example Question

Let $f(x) = x \oplus 1^n$ which of the following claims are true? (Circle all that apply)

A. f is a permutation

B. f is collision resistant

C. f is one-way

Example Question

Let F_K be a secure PRF which of the following claims are *necessarily* true? (Circle all that apply)

A. G(X) = $F_x(0^n) \| F_x(10^{n-1})$ is a secure PRG

B. G(X) = $F_{0^n}(x) \| F_{10^{n-1}}(x)$ is a secure PRG

C. G(X) = $F_x(0^n) \| F_y(10^{n-1})$ is a secure PRG here y = $F_x(0^n)$

D. f(x,k) = $k \| F_k(x)$ is a one-way function

E. f(x) = $F_x(0^n)$ is a one-way function

Next Class

- Midterm