Introduction to Cryptology ENEE459E/CMSC498R: Midterm Review Sheet

1 Overview

The midterm exam will be held during class on 3/15/18. It is closed book, closed notes, no calculators, cell phones, laptops.

2 Sections Covered

The exam will cover the following Sections from the textbook:

- Chapter 1: Sections 1.1, 1.2, 1.3
- Chapter 2: Sections 2.1, 2.2, 2.3, Shannons Theorem from Section 2.4.
- Chapter 3: Sections 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7
- Chapter 4: Sections 4.1, 4.2, 4.3, 4.4, 4.5

There will be a cheat sheet attached to the exam which will include the following information:

- Definitions of Perfect Secrecy.
- Shannon's Theorem.
- Definitions for indistinguishable encryptions in the presence of an eavesdropper and CPA-security.
- Definitions for pseudorandom generator and pseudorandom functions.
- Pictures for Cipher Block Chaining (CBC), Output Feedback (OFB) and Counter (CTR) Modes of Operation.
- Definition for (strong) unforgeability for MACs.
- Picture for CBC MAC.
- Definitions for Authenticated Encryption (CCA security and Unforgeability).

3 Practice Problems

3.1 Perfectly Secret Encryption

1. Give an example of an encryption scheme where $|\mathcal{K}| \geq |\mathcal{M}|$, but the encryption scheme is not perfectly secret.

2. Assume an encryption scheme has the property that for every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$, there is exactly one key $k \in \mathcal{K}$ such that $\mathsf{Enc}_k(m) = c$. Is this encryption scheme necessarily perfectly secret? Justify your answer.

3. For each of the following encryption schemes, state whether the scheme achieves perfect secrecy. Justify your answer using Definitions 2.1 and/or Lemmas 2.2, 2.3.
   (a) Message space $\mathcal{M} = \{0, 1, \ldots, p1\}$. Key space $\mathcal{K} = \{0, 1, \ldots, p1\}$, for prime $p > 2$. $\mathsf{Gen}()$ chooses a key k at random from $\mathcal{K}$. $\mathsf{Enc}_k(m)$ returns $m + 2k \mod p$. $Dec_k(c)$ returns $c2k \mod p$.

   (b) Message space $\mathcal{M} = \{0,1\}^n$. Key space $\mathcal{K} = \{0,1\}^n$. $\mathsf{Gen}()$ chooses a key k at random from $\mathcal{K}$. $\mathsf{Enc}_k(m)$ returns $c_1||c_2 = m \wedge k||m \vee k$, where $\wedge$ denotes bit-wise AND and $\vee$ denotes bitwise OR. $\mathsf{Dec}_k(c_1||c_2)$ computes the i-th bit of m in the following way: If the i-th bit of k is 0, return the i-th bit of c_2. If the i-th bit of k is 1, return the i-th bit of c_1.

3.2 Pseudorandom Generators and Indistinguishable Encryptions in the Presence of an Eavesdropper

1. Let G be a pseudorandom generator. Consider the following encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$: $\mathsf{Gen}(1^n)$ returns a secret key SK uniformly at random from $\{0,1\}^n$. $Enc_{sk}(m)$ chooses r at random from $\{0,1\}^n$ and returns $(r, G(\mathrm{SK}||r) \oplus m)$. $Dec_{sk}(c = (r, c_1))$ returns $G(\mathrm{SK}||r) \oplus c_1$. Does this encryption scheme necessarily have indistinguishable encryptions in the presence of an eavesdropper?

2. Consider the following construction of a pseudorandom generator G^* from a pseudorandom generator G : $G^*(s) = \overline{G(s)}$, where $\overline{G(s)}$ denotes bit-wise negation of $G(s)$. If G is a secure pseudorandom generator, then so is G^*. This can be proved by reduction: Given a distinguisher D breaking the security of G, we can construct a distinguisher D breaking the security of G. Specify the code of the distinguisher D (which uses D^* as a subroutine).

3.3 Pseudorandom Functions and Permutations and CPA-secure Encryption

1. Consider the following construction of an encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ from a pseudorandom function: $\mathsf{Gen}(1^n)$ returns a secret key SK uniformly at random from $\{0,1\}^n$. $\mathsf{Enc}_{\mathrm{SK}}(m)$ chooses r at random from $\{0,1\}^{n/2}$ and returns $(r, F_{\mathrm{SK}}(r||r) \oplus m)$. $\mathsf{Dec}_{\mathrm{SK}}(c = (r, c_1))$ returns $F_{\mathrm{SK}}(r||r) \oplus c_1$. Is the encryption scheme Π CPA-secure? Justify your answer.

2. Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a pseudorandom function. For all $\mathrm{SK} \in \{0,1\}^n$ and for all input $x \in \{0,1\}^{2n}$, define $F'_{\mathrm{SK}}(x_1||x_2) = F_{\mathrm{SK}}(x_1)||F_{\mathrm{SK}}(x_2)$. Is F' necessarily a pseudorandom function?

3. Consider the following variant of counter mode encryption: To encrypt a message $M = m_1, m_2, \ldots,$ where each $m_i \in \{0,1\}^n$, using key SK, choose a uniform $\mathsf{ctr} \in \{0,1\}^n$ and output the ciphertext

$$\mathsf{ctr}||F_{\mathrm{SK}}(\mathsf{ctr}+1+m1)||F_k(\mathsf{ctr}+2+m_2)||\cdots$$

   Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

4. Define an encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ such that Π has indistinguishable encryptions in the presence of an eavesdropper, but the entire secret key can be recovered via a CPA-attack.

3.4 Message Authentication Codes

Let F be a pseudorandom function. Show that each of the following message authentication codes is insecure. (In each case the shared key is a random $k \in \{0,1\}^n$.)

1. To authenticate a message $m = m_1||\cdots||m_\ell$, where $m_i \in \{0,1\}^n$, compute $t := F_k(m_1 \oplus \cdots \oplus m_\ell)$.

2. To authenticate a message $m = m_1||m_2$, where $m_1, m_2 \in \{0,1\}^n$, compute $t := F_k(m_1 \oplus m_2)||F_k(m_2 \oplus F_k(m_1))$.

3. We explore what happens when the basic CBC-MAC construction is used with messages of different lengths.

   (a) Say the sender and receiver do not agree on the message length in advance, but the sender is careful to only authenticate messages of length $2n$. Show that an adversary can forge a valid tag on a message of length $4n$.

   (b) Say the receiver only accepts 3-block messages, but the sender authenticates messages of any length a multiple of n. Show that an adversary can forge a valid tag on a new message.

3.5 CCA security and Authenticated Encryption

1. Let F be a strong pseudorandom permutation, and define the following fixed-length encryption scheme: On input a message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^n$, algorithm Enc chooses a uniform $r \in \{0,1\}^{n/2}$ and computes $c := F_k(m||r)$. Prove that this scheme is CCA-secure, but is not an authenticated encryption scheme.

2. Show a CPA-secure private-key encryption scheme that is unforgeable but is not CCA-secure.