Introduction to Cryptology ENEE459E/CMSC498R: Midterm Review Sheet

1 Overview

The midterm exam will be held during class on 3/10/16. 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
- Chapter 4: Sections 4.1, 4.2, 4.3

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

- 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.
- Definitions for existential unforgeability in the presence of an adaptive chosen message attack and strong unforgeability.

3 Practice Problems

3.1 Perfectly Secret Encryption

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

2. Assume an encryption scheme has the property that for every message $m \in M$ and every ciphertext $c \in C$, there is exactly one key $k \in K$ such that $\text{Enc}_k(m) = c$. 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 $M = \{0, 1, \ldots, p1\}$. Key space $K = \{0, 1, \ldots, p1\}$, for prime $p > 2$. $\text{Gen}()$ chooses a key $k$ at random from $K$. $\text{Enc}_k(m)$ returns $m + 2k \mod p$. $\text{Dec}_k(c)$ returns $c2k \mod p$.

   (b) Message space $M = \{0, 1\}^n$. Key space $K = \{0, 1\}^n$. $\text{Gen}()$ chooses a key $k$ at random from $K$. $\text{Enc}_k(m)$ returns $c_1 || c_2 = m \land k || m \lor k$, where $\land$ denotes bit-wise AND and $\lor$ denotes bitwise OR. $\text{Dec}_k(c_1 || c_2)$ 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 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$: $\text{Gen}(1^n)$ returns a secret key $SK$ uniformly at random from $\{0,1\}^n$. $\text{Enc}_{sk}(m)$ chooses $r$ at random from $\{0,1\}^n$ and returns $(r, G(SK||r) \oplus m)$. $\text{Dec}_{sk}(c = (r, c_1))$ returns $G(SK||r) \oplus c_1$. 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 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ from a pseudorandom function: $\text{Gen}(1^n)$ returns a secret key $SK$ uniformly at random from $\{0,1\}^n$. $\text{Enc}_{sk}(m)$ chooses $r$ at random from $\{0,1\}^{n/2}$ and returns $(r, F_{sk}(r||r) \oplus m)$. $\text{Dec}_{sk}(c = (r, c_1))$ returns $F_{sk}(r||r) \oplus c_1$. Is the encryption scheme $\Pi$ CPA-secure? Justify your answer.

2. Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a pseudorandom function. For all $SK \in \{0,1\}^n$ and for all input $x \in \{0,1\}^{2n}$, define $F'_sk(x_1||x_2) = F_{sk}(x_1)||F_{sk}(x_2)$. 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 $\text{ctr} \in \{0,1\}^n$ and output the ciphertext

$$\text{ctr}||F_{sk}(\text{ctr} + 1 + m_1)||F_k(\text{ctr} + 2 + m_2)||\cdots$$

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

4. Define an encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ such that $\Pi$ 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 $t := F_k(m_1 \oplus m_2)||F_k(m_2 \oplus F_k(m_1))$. 

2