Cryptography ENEE/CMSC/MATH 456: Final Review Sheet

1 Overview

The final exam will be held on Monday, 5/20/19 from 1:30pm-3:30pm in CSI 3117 (our regular classroom). It is not cumulative. It is closed book and notes. No calculator, cell phone or mobile devices.

2 Sections Covered

The exam will cover the following Sections from the textbook:

- Chapter 5: 5.1, 5.2, 5.3.1
- Chapter 6: 6.1, 6.2, 6.3
- Chapter 8: 8.1, 8.2, 8.3
- Chapter 10: 10.3
- Chapter 11: 11.2, 11.4, 11.5
- Chapter 12: 12.2, 12.4, 12.7, 12.8

In addition, the exam will cover the material on *post-quantum cryptography* covered in Lectures 25 and 26 on 5/6/19 and 5/8/19.

The following is a list of general topics focused on in the final exam and several practice problems for each topic.

3 Practice Problems

3.1 Collision Resistant Hash Functions

1. For each of the following modifications to the Merkle-Damgard transform, denoted H^s, determine whether the result is collision resistant. Justify your answer.
   (a) Instead of setting $z_0 := IV$, where IV is the initialization vector, set $z_0 := x_1$ to be equal to the first block of the message, and for $i > 0$, set $z_i := h^s(z_{i-1}||x_{i+1})$ (i.e. first h^s is called on input $z_0||x_2 = x_1||x_2$, yielding output z_1; then on input $z_1||x_3$ yielding output z_2, then on input $z_2||x_4$ yielding output z_3, etc.).
   (b) On input message m consisting of L bits, split $m = m'||m''$ into two parts of length $\lceil \ell/2 \rceil$ bits and $\lfloor \ell/2 \rfloor$ bits, respectively. Output $H^s(m')||H^s(m'')$.

3.2 Practical Constructions of Symmetric Key Primitives

1. In this question, you are asked to recover the first round key for a 1-round SPN with 6-bit input, 6-bit output and two 6-bit round keys, given two input-output pairs. Make sure to show all work.
   The SPN has the following structure:

   To compute the permutation $F_k(x)$ on input x (6 bits) with key k (12 bits):
   - Parse $k = k^1||k^2$, where k^1 and k^2 are the round keys and each have length 6 bits.
   - Compute the intermediate value $z = x \oplus k^1$.
   - Parse $z = z_1||z_2$, where z_1 and z_2 each have length 3 bits.

- For each $i \in [2]$, input z_i to the corresponding S-box S_i defined below, obtaining outputs w_1, w_2. Let $w = w_1||w_2$ (length 6 bits) be the combined output.
- Permute the bits of w to obtain w' as described in the chart below.
- Output $y = w' \oplus k^2$.

S-box S_1:

000	100
001	111
010	010
011	000
100	011
101	101
110	001
111	110

S-box S_2:

000	110
001	111
010	011
011	101
100	000
101	010
110	100
111	001

The following chart shows how the 6 bits of w are permuted to obtain w'.

1	2	3	4	5	6
3	4	5	6	1	2

Namely, on input $w := w_1, w_2, w_3, w_4, w_5, w_6$, we permute the bits to obtain output $w' := w_3, w_4, w_5, w_6, w_1, w_2$.
Assume you are given that $F_k(000000) = 111000$ and $F_k(111111) = 001111$. Let $k^1 := k^1_1, \ldots, k^1_6$.
You are additionally given that $k^2_2 = 0$ and that $(k^1_1||k^1_2||k^1_3) \oplus (k^1_4||k^1_5||k^1_6) = 110$. Find k^1 (first round key only).
Given the above information, there is an attack that requires you to evaluate the SPN at most 12 times. Solutions that recover the correct key but take longer, may not receive full credit.

2. Assume an SPN with block length 128. Moreover, assume there is no permutation step—only substituion steps and assume the same key schedule as our example in class (i.e. for an n-round network, $k = k_1, \ldots, k_n$ and the i-th part of the key is used in round i). How many round substitution network can you recover the entire key for in time 2^{40}.

3. Feistel network.
   (a) Consider a 1-round Feistel network where the round function is a PRF $F_k(\cdot)$. Is the function computed by the Feistel network a PRP?

   (b) Consider a 2-round Feistel network where the round function is a PRF $F_k(\cdot)$. Is the function computed by the Feistel network a PRP?

3.3 Number Theory

1. Let $N = p \cdot q$, for primes p, q. Assume $m \in Z_N \setminus Z_N^*$. Let e, d be such that $e \cdot d \equiv 1 \mod \phi(N)$. What happens when we compute $(m^e)^d \mod N$?

   Hint: Recall that $\phi(N) = (p-1)(q-1)$ and consider what happens when we compute $(m^e)^d \mod p$ and $(m^e)^d \mod q$ and then use CRT.

2. Use CRT and Fermat's Little Theorem to prove that for $N = p \cdot q$, where p, q are prime and $x \in Z_N^*$, $x^{\phi(N)} \equiv 1 \mod N$.

3. Extend CRT to the case where $N = p \cdot q \cdot r$ and p, q, r are prime. Namely, show how to solve for the unique $x \mod N$, given $a \equiv x \mod p$, $b \equiv x \mod q$ and $c \equiv x \mod r$.

4. The Euclidean Algorithm can also be used to find the gcd of two *polynomials*. Use the Euclidean Algorithm to find the gcd of the polynomials $p_1(x) = 3x^4 + 3x^3 - 17x^2 + x - 6$ and $p_2(x) = 3x^2 - 5x - 2$. Show your work.

5. Let p be a prime greater than 3 such that $p \mod 4 = 3$ (i.e. $p = 4m + 3$ for some positive integer m). Let $y \equiv x^2 \mod p$ for some integer x. Show how to find x, given y and p. In other words, you are showing how to find the square root of $y \mod p$.
   Use the fact that $(x^2)^{m+1} \equiv x^{2m+1} \cdot x \mod p$ and $(x^2)^{\frac{p-1}{2}} \equiv 1 \mod p$.

3.4 Key Exchange and Public Key Encryption

1. Consider the following key-exchange protocol: Common input: The security parameter 1^n. The protocol:
   (a) Alice runs $\mathcal{G}(1^n)$ to obtain (G, q, g).
   (b) Alice chooses $x_1, x_2 \leftarrow Z_q$ and sends $h_1 = g^{x_1 + x_2}$ to Bob.
   (c) Bob chooses $x_3 \leftarrow Z_q$ and sends $h_2 = g^{x_3}$ to Alice.
   (d) Alice outputs $h_2^{x_1+x_2}$. Bob outputs $h_1^{x_3}$.
   Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e. either prove its security or show a concrete attack).

2. Let (N, e) be the public key for plain RSA, where $N = 3 \cdot 11 = 33$ and $e = 3$. Find the corresponding secret key (N, d). Then encrypt the message $m = 16$, obtaining some ciphertext c. Decrypt c to recover m. Do the computations by hand and show your work.

3. Consider the subgroup of Z_{23}^* consisting of quadratic residues modulo 23. This group consists of the following elements: $\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. We choose $g = 3$ to be the generator of the subgroup. Let $(23, 11, 3, x = 4)$ be the secret key for ElGamal. Find the corresponding public key. Then encrypt the message $m = 9$, obtaining some ciphertext c. Decrypt c to recover m. Do the computations by hand and show your work.

4. Let $\text{PK}_1 = (N_1, 3), \text{PK}_2 = (N_2, 3), \text{PK}_3 = (N_3, 3)$, where $N_1 = 51, N_2 = 65, N_3 = 77, e = 3$. Assume a sender used plain RSA encryption to encrypt the same message m under public keys $\text{PK}_1, \text{PK}_2, \text{PK}_3$ to yield ciphertexts $c_1 = 2, c_2 = 57, c_3 = 50$. Find the message m by using the Chinese Remainder Theorem and solving for m. (See here for information on the Chinese Remainder Theorem `http://en.wikipedia.org/wiki/Chinese_remainder_theorem#A_constructive_algorithm_to_find_the_solution`).

5. Show that Textbook RSA and ElGamal encryption are "homomorphic." This means that given an encryption of a message m_1 and an encryption of a message m_2, we can multiply them to get an encryption of the message $m_1 \cdot m_2$. Is this property good or bad for security? Justify your answer.

3.5 Digital Signatures

1. Another approach (besides hashing) that has been tried to construct secure RSA-based signatures is to *encode* the message before applying the RSA permutation. Here the signer fixes a public encoding function $enc : \{0,1\}^{\ell} \to Z_N^*$ as part of its public key, and the signature on a message m is $\sigma := [enc(m)^d \mod N]$.

   (a) Show that encoded RSA is insecure if $enc(m) = 0x00||m||0^{\kappa/10}$ (where $\kappa = ||N||, \ell = |m| = 4\kappa/5$, and m is not the all-0 message). Assume $e = 3$.

   (b) Show that encoded RSA is insecure for $enc(m) = 0||m||0||m$ (where $\ell = |m| = (||N|| - 1)/2$ and m is not the all-0 message). Assume $e = 3$.

3.6 Post Quantum Cryptography

1. Let Λ be the lattice consisting of vectors $x \in \mathbb{Z}^m$ such that $Ax = 0 \mod p$, where A is a randomly chosen matrix $A \in \mathbb{Z}^{n \times m}$ and $m > n$. Find a basis B for the lattice Λ.

2. Find the n number of $2n$-primitive roots $\gamma_1, \ldots, \gamma_n$ modulo q, where $n = 8$, $q = 17$.

3. Consider the ring $R_q := Z_q[x]/x^n + 1$, where $n = 8, q = 17$. Show how to multiply the polynomials $p_1(x) = 13x^7 + 10x^6 + 5x^5$ and $p_2(x) = 11x^2 + 7x + 13$ using polynomial multiplication over R_q and using the NTT transform.