Cryptography ENEE/CMSC/MATH 456: Final Review Sheet

1 Overview

The final exam will be held on Monday, 5/18/20 from 1:30pm-3:30pm (Canvas submissions will be accepted until 4pm). It is not cumulative. It is open book and notes. I will also post a cheat sheet.

2 Sections Covered

The exam will cover the following Sections from the textbook:

- Chapter 5: 5.1.2, 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

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 Domain Extension for 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) Given an input/output pair $(L_0, R_0), (L_3, R_3)$, determine the constraints induced on the round function F_k (assume that the same round function F_k is used in all three rounds).

   (b) Given three input/output pairs $(L_0, R_0), (L_3, R_3), (L_0 + \Delta, R_0), (L'_3, R'_3), (L''_0, R''_0), (L_3, R_3 + \Delta)$ determine the constraints induced on the round function F_k (assume that the same round function F_k is used in all three rounds). What goes wrong?

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 $N = p \cdot q$ be a product of distinct primes. Show that every perfect square modulo N has 4 square roots.

   Hint: Use CRT and the fact that every perfect square modulo p (respectively, q) has exactly two square roots $x, p - x$, which are negations of each other modulo p (respectively q).

6. Let $N = p \cdot q$ be a product of distinct primes. Show that an algorithm A for computing square roots modulo N can be used to factor N.

   Hint: Choose $x \leftarrow Z_N^*$ and run $A(x^2)$. With probability $1/2$, A will output a value y such that $y^2 = x^2$ but $y \neq x$ and $y \neq N - x$. In this case, show how x, y can be used to factor N.

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. Assume that p, q are Fermat primes (see here: `https://en.wikipedia.org/wiki/Fermat_number`). Explain why RSA cannot be hard for modulus $N = p \cdot q$.

3. 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.

4. 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.

5. 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.
6. 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 $E : \{0,1\}^\ell \to Z_N^*$ as part of its public key, and the signature on a message m is $\sigma := [E(m)^d \mod N]$.

   (a) Assume $e = 3$. Show that encoded RSA is insecure if $E(m) = 1||m||0^{\kappa-\ell-1}$, where $\kappa = |N|$, $|m| = \ell > (\kappa+2)/2$, $\kappa - \ell - 1$ is a multiple of 3 and it is required that $1 \cdot 2^{\kappa-1} + m \cdot 2^{\kappa-\ell-1} < N$.

   Hint: Consider choosing m such that $7N/8 < E(m) < 7N/8 + 2^{\kappa-\ell-1}$, which means that $2^\ell < 8E(m) - 7N < 2^\ell + 2^{\kappa-\ell+2}$. Then convert $8E(m) \mod N$ to the correct format by multiplying by $2^{\kappa-\ell-1}$.