Cryptography ENEE/CMSC/MATH 456: Final Review Sheet

1 Overview

The final exam will be held on Wednesday, 5/15/24 from 1:30pm-3:30pm in CHE 2118 (our regular classroom). It is not cumulative. It is closed book and notes. I will post the cheat sheet that will be given to you during the exam.

2 Sections Covered

The exam will cover the following Sections from the textbook:

- Chapter 7: 7.2, 7.3
- Chapter 9: 9.1, 9.3
- Chapter 11: 11.3
- Chapter 12: 12.2, 12.4
- Chapter 13: 13.2, 13.4, 13.6, 13.7

It will also cover the post-quantum unit (Lectures 23 and 24).

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 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 substitution 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. Assume a balanced 2-round Feistel network with input/output length of n. Further, assume the round functions are truly random functions. Assume one is given random input/output pairs $(x_1, y_1), \ldots, (x_t, y_t)$. How large does t need to be in order to distinguish the output of the Feistel network from a truly random permutation? Justify your answer.

3.2 Number Theory

1. Give a formal proof that Z^*_p is a group with respect to multiplication modulo p. In particular, we did not prove the closure property in class.

2. 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.

3. Recall the discrete log assumption is believed to hold in the group $\mathbb{Z}^*_p$, where p is a sufficiently large prime. However, given g^x, where g is a generator, there is a way to determine the least significant bit of x. Explain how this can be done. Is there a way to recover more bits of x, assuming the prime p has a certain structure? For example, what happens if p is a Fermat prime (prime number of the form $p = 2^k + 1$)?

4. Consider a cyclic group G of prime order q with generator g, and assume there is an adversary A running in time t for which

$$\Pr[A([g^x) = x] = 0.01,$$

where the probability is taken over uniform choice of $x \in Z_q$. (Note that A solves the discrete logarithm problem, but only with 1% probability over choice of x.) Show that it is possible to construct an adversary A' for which

$$\Pr[A'(g^x) = x] = 0.99$$

for all x. The running time t' of A' should be polynomial in t and $\log(q)$.

Hint: Use the fact that $\mathbf{Dlog}_g(y \cdot g^r) = (\mathbf{Dlog}_g(y) + r) \mod q$.

3.3 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. 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.

3. Let $\mathrm{pk}_1 = (N_1, 3), \mathrm{pk}_2 = (N_2, 3), \mathrm{pk}_3 = (N_3, 3)$, 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 $\mathrm{pk}_1, \mathrm{pk}_2, \mathrm{pk}_3$ 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.
4. Show that ElGamal encryption is "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.

3.4 Digital Signatures

1. What happens to the security of Schnorr's signature scheme if the Signer chooses the same value k twice when generating two signatures for two different messages? Either justify why the scheme remains secure, or provide an attack on the signature scheme in this case.

2. One reason Schnorr's signatures are popular in Bitcoin is the ability to aggregate signatures. I.e. these are settings in which there are two (or more) parties P_1, P_2. P_1 signs m under secret key x_1 and public key y_1, P_2 signs m under secret key x_2 and public key y_2. The signature is aggregated, and can be verified under public key $y = y_1 \cdot y_2$. Consider the following aggregate signature construction on input message m:
   - P_1, P_2 choose $k_1, k_2 \leftarrow Z_q$ and construct $I_1 = g^{k_1}, I_2 = g^{k_2}$.
   - $r = H(I_1 \cdot I_2 || m)$
   - P_1, P_2 compute $s_1 = k_1 + r \cdot x_1$, $s_2 = k_2 + r \cdot x_2$.
   - The combined signature is $(r, s_1 + s_2)$.

   Explain how the signature is verified and show the correctness of the above aggregate signature. Show that the above aggregate signature is insecure. Specifically, given a target y_2 (owned by a legitimate party), an attacker can create a "fake" y_1 and sign a message under $y = y_1 \cdot y_2$.

3.5 Post-Quantum Cryptography

1. Consider the lattice $\Lambda(B) \subseteq \mathbb{R}^3$ with basis B where

$$B = \begin{bmatrix} 1 & 1 & -4 \\ -2 & 2 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

   Note that the vectors in the basis B are orthogonal (the dot-product of every pair of column vectors is 0). Given this, what is the shortest vector in the lattice $\Lambda(B)$? Provide another basis B' that generates the same lattice (i.e. provide a matrix B' such that $\Lambda(B') = \Lambda(B)$) but for which the vectors in B' are not orthogonal. Why is it harder to find the shortest vector of the lattice given basis B' rather than basis B?

2. Consider the following two distributions:
   - $\mathcal{D}_1$: The uniform distribution over the set $\{0, \ldots, 8\}$.
   - $\mathcal{D}_2$: The distribution that corresponds to the random variable $Z = X + Y$, where X, Y are each chosen uniformly and independently from $\{0, \ldots, 4\}$.

   Explain how one could generate random samples from $\mathcal{D}_1$ and use rejection sampling to output random samples from $\mathcal{D}_2$. What is the expected number of samples one would need to sample from $\mathcal{D}_1$ in order to output a single sample from $\mathcal{D}_2$?