Introduction to Cryptology ENEE459E/CMSC498R: Final Review Sheet

1 Overview

The final exam will be held on Monday, 5/18/15 from 10:30am-12:30pm in ITV 1100 (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 4: 4.1, 4.2, 4.3, 4.4, 4.5
- Chapter 5: 5.1, 5.2, 5.3
- Chapter 6: 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, 12.5, 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 Message Authentication Codes and Collision-Resistant Hash Functions

1. 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.

2. Assume collision-resistant hash functions exist. Show a construction of a fixed-length hash function (Gen, h) that is *not* collision resistant, but such that the hash function (Gen, H) obtained from the Merkle-Damgard transform to (Gen, h) *is* collision resistant.

3.2 Practical Constructions of Symmetric Key Primitives

1. 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}.

2. 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 $(m^e)^d \mod q$.

2. Recall that the discrete logarithm problem is believed to be hard relative to the cyclic group Z_p^*, for prime p. Let g be a generator of Z_p^*. Nevertheless, show that, given g^x, it is possible to determine the least significant bit of x.

3. 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.

3.4 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`).

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

   (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 $e = 3$.