CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Midterm Exam

November 15, 2012

Question 1. (*40 pts.*) Answer briefly each of the following questions:

a. What is Kerckhoffs' principle? Why is that principle important?

b. What are the four basic operations in the AES round function? Which are responsible for confusion? Which are responsible for diffusion?

c. In general, the decryption speed of a block cipher algorithm is considered to be less important than its encryption speed. Why?

d. In which of the ECB, CBC, OFB, CFB, and CTR modes of operation, is speeding up *encryption* possible by precomputation? By parallel computation?

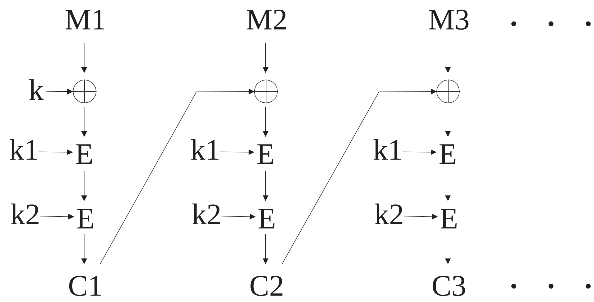
e. For a hash function, does collision resistance imply second preimage resistance? Explain briefly.

f. What is the existential forgery attack against textbook RSA signatures? How does PKCS (v1) solve this problem?

g. What is "key escrow"? Why is it an inherent feature in ID-based encryption?

h. What is the limitation of a simple secret sharing system that function sharing aims to solve? Discuss briefly.

Question 2. (*20 pts.*) Consider the following mode of encryption with three keys k, $k1$, $k2$, where k is of the length of the block size and $k1$ and $k2$ are of the length of the key size (denoted by ℓ) of the block cipher E. (E.g., for DES, k would be 64 bits, and $k1$ and $k2$ would be 56 bits each.)



a. Describe the decryption operation for this mode of encryption.

b. Describe a known-plaintext attack with a few input blocks where the attacker can discover the full key $(k, k1, k2)$ with approximately $2 \cdot 2^{\ell}$ runs of the encryption/decryption algorithm. (You can assume as much memory as you need for the attack.)

c. Comment on the security of this mode of encryption as a potential way of strengthening DES with an increased key size.

Question 3. (*20 pts.*) Suppose that we want to develop a MAC scheme which is as secure as Triple-DES CBC-MAC and at the same time as efficient as Single-DES CBC-MAC. We come up with the following idea: Except the last plaintext block, we apply Single-DES CBC with key K_1 and for the last one, we apply 2-key Triple-DES CBC-MAC using keys (K_1, K_2, K_1). The result of the Triple-DES is output as the MAC.

a. Approximately how many message-MAC pairs would you need to observe in order to find two different messages with the same MAC value?

b. Describe how an attacker who has observed two different messages with the same MAC value can break this MAC scheme completely by recovering the keys with a time complexity about the same as that of breaking a Single DES encryption.

Question 4. (*20 pts.*) On ElGamal signatures. (You can assume that g has a prime order q.)

a. Show that if Eve can learn the value of k Alice used in an ElGamal signature, she can compute Alice's private key.

b. Suppose Alice's random number generator is broken and it always produces the same k value. How can Eve detect this from the signatures Alice issues?

c. Knowing that Alice used the same k value in two different signatures, describe how Eve can compute that k value used, and then Alice's private key α.

Good luck!