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

Midterm Exam

November 11, 2008

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

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

b. Is AES a Feistel cipher? Why/why not?

c. How is diffusion across s-boxes provided in the AES encryption function? Briefly explain the diffusion-related operations and their roles.

d. In which of the ECB, CBC, OFB, CFB, and CTR modes of operation, is speeding up the encryption by precomputation possible? Briefly describe how.

e. What is the message encryption and authentication mechanism in WEP? Describe how it fails completely. Would this attack still be possible if the CRC checksum is encrypted with a block cipher (say, AES) while the message is still encrypted with RC4? Why/why not?

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

g. What is the basic idea of ID-based encryption? Describe the key management structure needed to realize such a system.

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

Turn the page

Question 2. (*20 pts.*) The banking industry developed the "retail MAC" scheme to be an efficient and secure MAC with the security level of a Triple-DES CBC-MAC and the performance of a Single-DES CBC-MAC. The scheme works by applying Single-DES CBC computation with key K_1 throughout the message except for the final block, and for the final block a 2-key Triple-DES CBC-MAC is applied with keys (K_1, K_2, K_1). Assume that the result of the Triple DES computation is output as the MAC.

a. How many message-MAC pairs would you need to observe approximately 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 about the same time complexity of breaking a Single DES encryption.

Question 3. (*20 pts.*) A misuse of the ElGamal signature scheme is to use the same k value multiple times. Show that if Bob signs two different messages m_1, m_2 with the same k value and obtains the signatures (r, s_1), (r, s_2), Trudy can produce a valid signature for any message she likes. (Hint: First work by assuming $\gcd(s_1 - s_2, p-1) = 1$—or, equivalently, $\gcd(m_1 - m_2, p-1) = 1$. Then generalize your proof to arbitrary s_1, s_2.)

Question 4. (*20 pts.*) Consider a variant of the ElGamal signature scheme where $p, q, g, \alpha, \beta, k, r$ are as in the original scheme as described in class and

$$s = (1 - m\alpha)k^{-1}r^{-1} \bmod q.$$

a. What is the signature verification formula for this modified scheme?

b. Show that this ElGamal variant is completely insecure and an attacker can issue a forged signature even without seeing a previously signed message. (Hint: Assign a random number to the product rs.)

Good luck!