Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Midterm Exam

December 9, 2011

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

a. What is the major limitation of traditional substitution ciphers? How do the modern block ciphers address it?

b. What is the major limitation of the traditional one-time pad? How do the modern stream ciphers address it?

c. Which of the ECB, CBC, OFB, CFB, and CTR modes of operation allow starting the decryption at an arbitrary point of the encrypted data? Explain each briefly.

d. What are the differences between a MAC and a digital signature? What are the respective advantages of each?

e. What is the “guessable plaintext” problem in public key encryption? Does it also apply to ElGamal encryption? Why/why not?

f. Suppose all members in a group use 5 as their RSA encryption exponent. What is the risk of sending the same message to multiple members in such a system? How does PKCS (v1) solve this problem?

g. Establishing a secure channel between two previously unacquainted parties over an insecure network requires support from a trusted third party, either a KDC or a CA. What are the relative advantages of each approach?

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

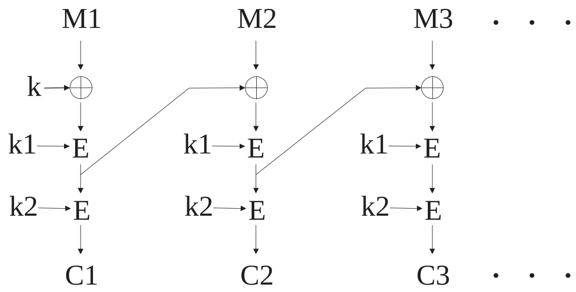
Turn the page

Question 2. (*20 pts.*) Let $\overline{x}$ denote the bitwise complement of a binary string x. Show that

$$DES_{\overline{K}}(\overline{P}) = \overline{C}$$

where $C = DES_K(P)$. Make sure that you mention the significance of the relevant DES features (i.e. key schedule, expansion, key mixing (XOR), confusion, diffusion, Feistel structure) as necessary.

Question 3. (*25 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 chosen-ciphertext attack where the attacker can discover the full key $(k, k1, k2)$ with $O(2^\ell)$ runs of the encryption/decryption algorithm. You can assume as much memory as you need for the attack. (Hint: Consider two ciphertext messages (C_1, C_2) and (C_1', C_2), for some randomly chosen C_1, C_2, C_1'.)

c. Would a similar *chosen-plaintext* attack work? Argue briefly.

Question 4. (*15 pts.*) Consider a variation of the ElGamal signature scheme where $p, g, \alpha, \beta, k, r$ are as in the original scheme as described in class and

$$s = (m - kr)\alpha^{-1} \bmod (p - 1).$$

a. What would the signature verification formula be for the modified scheme?

b. What is a computational advantage of the modified scheme over the original one?

Good luck!