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

Midterm Exam

November 18, 2002

Problem 1. (*40 pts.*) Answer briefly (i.e., in no more than four lines for each) 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) Is AES a Feistel cipher? Why/why not?

d) Which of the ECB, CBC, OFB, CFB, and CTR modes of operation allow starting the decryption at an arbitrary point of the encrypted data?

e) What are the differences between a MAC and a digital signature? What are the respective advantages of each?

f) An RSA signature operation $x^d \bmod n$ can be sped up by first computing x^d in Z_p and in Z_q and then getting the answer in Z_n by the Chinese Remainder Theorem. In this way, the size of both the bases and the exponents in the computations will be reduced. Can this optimization be also utilized for the public key encryption operation? Why/why not?

g) What is the "cube root problem" in RSA? How does the PKCS address it?

h) Establishing trust between two previously unacquainted parties over a network requires help from a trusted third party, either a KDC or a CA. How do KDC-based systems and CA-based systems compare in terms of scalability and trust?

Problem 2. (*20 pts.*) For $Y = DES_K(X)$, prove that $\bar{Y} = DES_{\bar{K}}(\bar{X})$, where $\bar{x}$ denotes the bit-wise complement of x. (Hint: Work by induction on the number of rounds.)

Turn the page

Problem 3. (*20 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? (put your answer in a frame)

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

Problem 4. (*20 pts.*) Alice uses the RSA algorithm for the authentication of her messages with the optimization technique described in Problem 1.f. That is, to sign a message x, she first computes $y_1 = x^d \bmod p$, $y_2 = x^d \bmod q$, and then obtains $y = x^d \bmod n$ by the Chinese Remainder Theorem. During the signature of a message, while y_1 was being computed, a glitch at Alice's computer caused it to produce a wrong value $\tilde{y_1}$ different from y_1. Then the computation of y_2 proceeded without any errors. At the end, a wrong signature $\tilde{y}$ was obtained from $\tilde{y_1}$ and y_2.

a) Show that any person who observes the message x with the wrong signature $\tilde{y}$ can factor Alice's modulus n. (Hint: Use the fact that $\tilde{y}^e \equiv x \pmod{q}$.)

b) Suggest some method by which Alice can defend against this danger.

Good luck