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

Midterm Exam

November 5, 2009

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

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

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

c. What is the weakness of generating the same key stream multiple times from the encryption key in a stream cipher? How is this solved in practice?

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

e. What is the "cube root problem" in RSA encryption? How does PKCS address it?

f. What is the main advantage of elliptic curve cryptosystems over RSA and ElGamal?

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 key revocation? Is ID-based or traditional certificate-based key management more suitable with regard to key revocation? Why?

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 $C = DES_K(P)$. (Hint: First prove the property for one round of DES. Then extend it to the whole cipher.)

Question 3. (*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?

Question 4. (*25 pts.*) In this exercise, you will prove that the CBC-MAC in its plain form is not secure to authenticate variable-length messages.

a. Consider the CBC-MAC scheme with an n-bit block cipher where the CBC checksum of a message is calculated with a zero IV. Describe an attack where an attacker Eve can construct the MAC of a message different from those she obtained from the legitimate sender. (Hint: Let the attacker obtain the MAC of two n-bit messages and from them compute the MAC of a $2n$-bit message.)

b. An attempt to solve this problem could be to append the number of blocks in the message as a final block to the message; i.e., to apply CBC on $(M\|b)$ instead of M alone, where b denotes the number of blocks in M. Show that this construction is not secure either. (Hint: Let the attacker obtain the MAC of some more messages.)

c. How about prepending the number of blocks; i.e., to apply CBC on $(b\|M)$? Does a similar attack work on this construction as well? How would its performance compare to the appending scheme of part (b)?

Good luck!