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

Midterm Exam

November 9, 2010

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. Consider using the CBC decryption operation for encryption. Why wouldn't this be a secure mode of encryption?

c. The decryption speed of a block cipher may not be as important as the encryption speed, it is argued in the Rijndael design document. Why not? Explain briefly.

d. What is the risk of using the same k value multiple times in ElGamal encryption? Discuss briefly.

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

h. What is function sharing? What is its advantage over simple secret sharing?

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 relevant DES features as necessary.

Question 3. (*20 pts.*) Consider the following MAC scheme with a 128-bit block cipher, similar to the CTR mode of encryption:

- Append a 1 bit to the message, and then enough 0 bits to make the total length of the message a multiple of 128 bits.
- Break the message into 128-bit blocks; $M_1, M_2, \ldots$.
- Encrypt independently each block M_i as $C_i = E_K(M_i) \oplus E_K(i)$.
- Take the low-order two bytes of each ciphertext block C_i. Concatenate them, yielding the final MAC.

(Note that this is a variable-length MAC.)

a. Why is the padding done the way it is rather than just padding the last block with 0 bits?

b. Show that this MAC is not secure by a simple truncation attack. (I.e.: The attacker observes a message M and its MAC $MAC_k(M)$. Then he obtains the MAC of another message M', which is a truncation of M.)

c. Describe another attack on this MAC scheme where the attacker computes the MAC of a message without having the MAC of any other messages beforehand.

Question 4. (*20 pts.*) In an RSA-based secure communications system, it may be desirable to simplify the key generation and management process by using a system-wide common modulus N, generated by a trusted key generation authority, and user-specific key pairs (e, d). Show that such a common-modulus system is totally insecure against insider attacks by proving the following steps:

a. Eve, possessing a key pair (e_E, d_E), can easily compute a multiple of $\varphi(N)$, say $k \cdot \varphi(N)$.

b. If Alice's public key e_A is relatively prime to k, Eve can find a decryption exponent for Alice and read all her messages.

c. Eve can compute a decryption exponent for any user in the system, whether or not $\gcd(e, k) = 1$.

Good luck!