CS 4476(5413) MID TERM EXAMINATION

February 27, 2008

Duration: One hour

Name:

Student Number:

Note: Each student needs to solve 6 problems. Every student should solve all the problems in Set A. For students of CS 4476, choose 3 problems in Set B and 1 problem in Set C. For students of CS 5413, choose 2 problems from Set B and 2 problems from Set C. If you solved more than 6 problems, please indicate which of the solutions you want to be marked.

Set A

Problem 1.

Do you agree the following statements? Give brief reasons to support your opinion. (Note: If you agree a statement, then it means that you agree all the sentence(s) in that statement.)

1. The statistical methods can be used to attack mono-alphabetic encryptions, because the appearances of English letters in texts have fixed distributions. But these methods are useless for attacking the encryption of binary files.

2. Substitution methods are used in both DES and AES, because Substitution Cipher is a secure encryption method.

3. Public key encryptions are not very efficient, because they are more secure than block cipher.

4. In RFC standard, RFC means Request For Comments.

5. Both public key systems and secret key systems can be used to distribute keys.

Problem 2.

Suppose Bob has an RSA public key system as follows: The public keys are $n = 33$ and $b = 3$, the private keys are $p = 3, q = 11$ and $a = 7$.

- If Alice wants to send a plaintext $x = 8$ to Bob using his public key, then what is the ciphertext?
- If Bob wants to sign a plaintext $x = 4$, then what is the signature?

Set B

Problem 3.

Suppose the following ciphertext is obtained by a Permutation Cipher of size 5 on 26 English letters plus space:

```
edrapmttnefooc pmetu ricsne ec
```

Find the plaintext.

Problem 4.

Suppose $e_K()$ is a block cipher. For a plaintext $x = x_1 x_2 \cdots x_n$, the CBC mode of encryption is:

$IV = y_0, y_1 = e_K(y_0 \oplus x_1), y_2 = e_K(y_1 \oplus x_2), \cdots$.

1. What is the purpose of defining an IV? Should it be kept in secret?
2. Explain why this mode is good for message integrate.
3. Is it good for communicating over a noisy channel? Why?

Problem 5.

1. Write down the algorithms of the Diffie-Hellman key exchange scheme.
2. How to use the man-in-the-middle attack for D-H key exchange?
3. If the discrete logarithm problem has an efficient solution, the the D-H key exchange scheme is broken. Explain why.

Problem 6.

1. What is the main purpose of certificates used in network security?
2. Should we use a certificate for the key of AES? Why?

Problem 7.

1. What are the security requirements for hash functions?
2. Why we cannot use a hash function to do encryption?
3. Why we can still use SHA-1 for one-time password even the SHA-1 was broken?

Set C

Problem 8.

Suppose Alice has an RSA system with public key (n_A, b_A), private key a_A and Bob has an RSA system with public key (n_B, b_B), private key a_B. Their public keys are certificated. Both of them has an AES algorithm and a SHA-224 algorithm. Alice wants to send several important files to Bob over the internet secretly. She is also wants to make sure that Bob receives these files correctly. Design communications between Alice and Bob for that purpose.

Problem 9.

The ElGamal cryptosystem is as follows. For $\beta \equiv \alpha^a \bmod p$ (where β, α and p are public), and a plaintext x, Alice chooses a secret random value k and sends Bob $(y_1, y_2) = (\alpha^k, x\beta^k) \bmod p$. Then Bob can computes $x = y_2(y_1^a)^{-1} \bmod p$. Suppose Alice sent x to Bob twice using this cryptosystem. At first time she used a random number k and at second time she used $2k$ as the secret random value. Do you think this method will cause problem? Explain why.

Problem 10.

Alice has an AES-128 encryption algorithm $E_K(x)$, where K is a key of 128 bits and x is a block of plaintext of 128 bits. She wants to use it to create a hash function as follows.

For a plaintext $x_1x_2\cdots x_n$ of n blocks of 128 bits, let K be 128 bits of 0 and compute:

$$O_1 = E_K(x_1), O_2 = E_K(x_2) \oplus O_1, \ \cdots\cdots \ , O_n = E_K(x_n) \oplus O_{n-1}.$$

The output is O_n. List all the deficiency of this hash function.