CS 4476(5413) MID TERM EXAMINATION

February, 2005

Duration: One hour

Name:

Student Number:

Note: Each student needs to solve 6 problems. Every student should solve 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 problems you want to be marked.

Set A

Problem 1.

Do you agree the following statements? Give brief reasons to support your opinion.

1. A public key encryption system is more secure than a secret key encryption system, but the former system is not as efficient as the later one.

2. The main purpose of PKI is to manage public key certificates.

3. A monoalphabetic cryptosystem is not secure, because probabilistc methods may break the system even under a cipher text only attack.

4. The main methods for checking whether a hash function is secure are examing whether the hash function is a one-way function (i.e., it is difficult to find the inverse of the function).

Problem 2.

Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, key space $\mathcal{K} = \{(a, b) : a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}\}$. Define the encryption function as

$$e_{(a,b)}(x) \equiv ax + b \pmod{26}.$$

Suppose $(a, b) = (9, 5)$ and the plaintext is `good`. What is the ciphertext? The correspondences between $\mathbb{Z}_{26}$ and English characters are as follows.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Set B

Problem 3.

One encryption method is as follows. Let m be an integer. Write the plaintext in a table with rows of length m. The ciphertext is obtained by taking the columns of the table. For example, when $m = 3$ and the plaintext is `networksecurity`, the table is:

```
net
wor
kse
cur
ity
```

So the ciphertext is `nwkcieosuttrery`. This is a special case of Permutation Cipher. Decrypt the ciphertext `imnrnpsinasiduetftetctcyoicyoeuorouamrro`. (Note here m is not necessary 3).

Problem 4.

Suppose Alice and Bob only have an AES encryption algorithm $e_K()$ and share a secret key K. Design a method (a mode) for them, which can be used for both encryption and decryption.

Problem 5.

Suppose Alice has an RSA system with public key (n_1, b_1) and private key (a_1, p_1, q_1), and Bob has an RSA system with public key (n_2, b_2) and private key (a_2, p_2, q_2). Alice wants to send Bob a message x using these systems to encrypt and authenticate. Indicate what should Alice do and what values should Alice send to Bob through the internet.

Problem 6.

Explain why birthday attack can be used to attack a hash function, but not suitable to use for attacking an public key encryption function.

Set C

Problem 7.

Alice suggested a simple MAC function to Bob as follows. Suppose Alice and Bob share a secret key K with length of at least 128 bits. For a message x of any length greater than 128 bits, define the MAC value as:

$$MAC_K(x) = x \bmod K.$$

Do you think this is a good MAC function? Explain why.

Problem 8.

Define a public key signature scheme as follows. Let

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \bmod p\}.$$

where p is a large prime and α is a primitive number of $\mathbb{Z}_p$. The values of p, α and β are public and a is secret.

For $K = (p, \alpha, a, \beta) \in \mathcal{K}$ and for a secret random number $k, 1 \leq k \leq p - 1$, the signature of a message $x \in \mathbb{Z}_p^*$ is

$$sig_K(x, k) = (\gamma, \delta),$$

where

$$\gamma = (\alpha^k \bmod p)$$

and

$$\delta = (x - k\gamma)a^{-1} \bmod p - 1.$$

Write down the verification algorithm for this signature scheme.

Problem 9.

Suppose Bob has an RSA public key system with the public key certificated. Both Alice and Bob have SHA-256 and AES algorithms. If Alice wants to communicate with Bob, then what should Alice do to let the communication efficient, secure, and authenticated?