UNIVERSITY OF LONDON 291 0326W

FOR EXTERNAL STUDENTS – WESTERN

B.Sc. EXAMINATION 2006

COMPUTING AND INFORMATION SYSTEMS

CIS326 Computer Security

Duration: 2 hours 15 minutes

Date and time: Thursday 11 May 2006: 2.30 - 4.45pm

Answer any **three** of the following five questions

Full marks will be awarded for complete answers to a total of three questions. Each question carries 25 marks. The marks for each part of a question are indicated at the end of the part in [ ] brackets.

There are 75 marks available on this paper.

Electronic calculators must not be programmed prior to the examination. Calculators which display graphics, text or algebraic equations are not allowed.

Answer any three of the following five questions. There are 25 marks for each question.

1. a) In a bank, the customers details are confidential, they are stored electronically and can only be accessed by authorized personnel entering their username and password.

i. Define what is meant by a *one-way* function and describe how a one-way function can be used to cryptographically protect the password file on the bank's computer system. [6]

ii. A hacker gains access to the encrypted password file. Describe how he might try to discover a password that will allow him access to the bank's computer system. [5]

iii. What steps should be taken by the bank in order to prevent the hacker from succeeding in his attack? [2]

b) In the loans department at the bank there are two secure sections *mortgages* and *credit cards*. Documents in this department are either concerned with mortgages, or with credit cards, or with both or with neither, and the security labels are respectively *{m}, {c}, {m,c}, and { }*.

i. Draw the directed graph for the security policy. [2]

ii. What security label would be assigned to the head of the loans department? [1]

iii. What security label would be assigned to a document concerned exclusively with mortgages? [1]

iv. What security label would you assign to the deputy head of credit card loans? [1]

v. Decide using your graph and previous answers whether or not the deputy head of credit card loans would have access to the document concerned exclusively with mortgages. [1]

c) In general, passwords should be relatively long to enhance security. However *PIN*s (personal identification number) used with credit cards, for example to draw money out of a cash machine, have only four decimal digits.

i. Why is it safe to have PINs of only four digits even though we would normally recommend that passwords are longer than this? [3]

ii. Suggest two ways in which a credit card user could make it harder for an attacker to find out their PIN. [3]

2. a) Explain why a good cryptosystem should have a large alphabet and a large keyspace. [2]

What is the alphabet and the keyspace for each of the following symmetric cryptosystems:

i. Caesar's cipher
ii. DES (Data Encryption Standard) [6]
iii. Triple-DES

b)

It is trivial matter for a cryptanalyst to break Caesars cipher. An improvement to that cryptosystem is to use a substitution alphabet based on a random permutation, rather than a simple rotation, of the letters.

i. If it takes a cryptanalyst using an exhaustive search technique *x* minutes to find the key used for the Caesars cipher, approximately how long will it take him to find the key used for the substitution cipher using the same technique? [2] [4]
ii. What methods could the cryptanalyst use to find the substitution key in a faster time? [4]
iii. Suggest how the substitution cipher could be improved to make it harder for the cryptanalyst to find the key.

c)

In modern applications, the AES symmetric cryptosystem Rijndael is sometimes used in favour of Triple DES. What are the advantages and disadvantages of Rijndael compared with Triple DES? [4]

d)

The *one-time pad* is the most secure of all symmetric key cryptosystems.

i. Explain how Alice and Bob can use a one-time pad to communicate securely.
ii. Why is the one-time pad so secure? [3]
iii. Why isn't the one-time pad used in all cryptosystems?

3. a) Four ways in which an attacker can disrupt a communication are *interruption, interception, modification* and *fabrication.*

Briefly describe each of these four attacks and suggest ways in which they could be detected. [8]

b) Alice and Bob have come up with an easy method for secretly communicating a number m.

- Alice chooses a secret number a
- Alice calculates $c_a = m+a$ and she sends c_a to Bob.
- Bob chooses a secret number b
- Bob calculates $c_{ab}=c_a+b$ and he sends c_2 to Alice
- Alice calculates $c_b=c_{ab}-a$ and she sends c_b to Bob.
- Bob calculates $m=c_b-b$

Discuss the security of this scheme. Are there any ways in which an attacker can disrupt this communication? [7]

c) Explain how the El Gamal public key cryptosystem can be used commutatively to exchange a message between Alice and Bob in a manner similar to that described in (b).

Illustrate your answer using the following keys and message $m=12$.

Alice: $p=19,\ g=2,\ a=7,\ y_a=2^7 \bmod 19=14,\ k_a=4$

Bob : $p=19,\ g=2,\ b=10,\ y_b=2^{10} \bmod 19=17,\ k_b=5$

[10]

The following table shows inverses mod 19 which you may need to help you with your answer.

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*
1	*10*	*13*	*5*	*4*	*16*	*11*	*12*	*17*	*2*	*7*	*8*	*3*	*15*	*14*	*6*	*9*	*18*

4. a) Describe the key generation process for the RSA public key cryptosystem. [6]

b) Alice has public and private RSA keys (n=91, e=11) and (d=59).
Bob has public and private RSA keys (n=170, e=23) and (d=7).

Assuming the role of Bob, and showing all your working, encrypt **and** sign the message m=20 to send to Alice. [8]

c) Give four essential properties of a cryptographic hash function. [2]

d) Describe the cryptographic hash function SHA-1 [4]

e) Write a protocol for digital signatures, which makes use of both SHA-1 and RSA. [5]

5. a) Describe the *X.509* certification process detailing:

i. how the Certification Agency provides a certificate for a user Alice; and
ii. how user Bob can verify that he has the correct public key for Alice. [6]

b) Name and describe a protocol which uses symmetric and public key cryptosystems to provide confidentiality but which does not make any use of certificates to authenticate public keys. [9]

c) Give one advantage and one disadvantage of using certificates to authenticate public keys. [2]

d) The Needham-Schroeder Protocol is a method of exchanging a session key between Alice and Bob using a trusted third party or server *S*. Alice and Bob each share a key with the server, but generate a new session key K_{AB} each time they want to communicate with each other. The keys that Alice and Bob share with the server are denoted by K_{AS} and K_{BS} respectively. The basic protocol can be written symbolically as follows:

1. Alice →S : A, B
2. S → Alice : $e_{KAS}(B, K_{AB}, e_{KBS}(A, K_{AB}))$
Alice decrypts
3. Alice → Bob : $e_{KBS}(A, K_{AB})$
Bob decrypts

Charles is a cryptanalyst who has access to all communications between Alice, Bob and Server. How does the protocol overcome the following problems:

i. Charles determining the session key K_{AB}?
ii. Charles masquerading as Alice?
iii. Charles masquerading as Bob?
iv. Charles preventing Bob from receiving any information from Alice?
v. Charles replaying a previous key generation? [8]

END OF EXAMINATION