UNIVERSITY OF LONDON 291 0326E

FOR EXTERNAL STUDENTS - EASTERN

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.

UL06/514

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

1. a) Exam papers are stored electronically and can only be accessed by authorized personnel.

i. Describe the process of identification and authentication using passwords. [2]

ii. Define what is meant by a one-way function and give an example of such a function. Describe how a one-way function can be used to cryptographically protect the password file. [6]

iii. The function used to protect a password file should be very efficient so that authorized personnel can log in without delay. Is this statement TRUE or FALSE? Give reasons for your answer. [3]

b) In a particular department, there are five lecturers *A, B, C, D* and *E*. Each lecturer has responsibility for setting an examination paper. Lecturer *A* sets paper *a*, lecturer *B* sets paper *b* and so on. All of the examination papers are checked by a different lecturer . This is done by rotating the papers, so lecturer *B* checks and corrects paper *a*, lecturer *C* checks and corrects paper *b*,....., and lecturer *A* checks and corrects paper *e*. Finally the Head of Department *H* reads each of the papers and comments on them directly to the lecturer who set the paper. The Head of Department does not herself make any changes on the examination papers.

Construct an access control policy for this system, stating the subject, objects and operations and writing down the access control matrix. Draw a lattice showing set inclusions for the operations you have defined. [10]

c) If a user has to remember several passwords at a time, he or she may consider storing them in a *password book*. A password book is a protected file that contains all of the passwords. Access to the password book can be controlled through a master password. What are the advantages and disadvantages of using a password book? [4]

2. a) A good cryptosystem should have a large alphabet and a large keyspace.

i. What are meant by the terms *alphabet* and *keyspace* in this context? Why is it important for a cryptosystem to have a large alphabet and a large keyspace? [4]

ii. Give another two properties of a good cryptosystem, explaining the importance of each. [4]

iii. State the size of the alphabet and the keyspace for the symmetric cryptosystems DES (Data Encryption Standard) and AES (Rijndael). [5]

b) Describe Triple DES in terms of DES and answer the following questions: [3]

i. If it takes x seconds to encrypt one block using DES, how long will it take to encrypt one block using Triple DES? [1]

ii. If it takes y seconds to transmit one block using DES, how long will it take to transmit one block using Triple DES? [1]

iii. If it takes cryptanalyst z hours to find the DES key using an exhaustive search technique, how long will it take him to find the Triple DES key using the same technique? [1]

c) In a *known-message attack* on a symmetric key cryptosystem, one strategy for a cryptanalyst is to try all of the possible keys, In a particular system the key consists of 64 binary bits.

i. If the cryptanalyst can try 10^{12} keys per second, will it take roughly 3 seconds, 3 minutes, 3 hours, 3 days, 3 weeks, 3 months or 3 years for him to find the key? Justify your answer. [3]

ii. What is the difference between a *known-message attack* and a *chosen-message attack*? What strategy might the cryptanalyst use in a chosen-message attack? [3]

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

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

b) Alice wishes to send Bob a valuable item that is locked inside a briefcase. The briefcase and padlock are tamper proof, but Alice has no way of getting a duplicate key to Bob. She therefore sends the briefcase to Bob with instructions for him to put on his own padlock and then return the briefcase with both padlocks on to Alice. On receiving the briefcase back from Bob, Alice removes her own padlock and then returns the briefcase to Bob. Bob can then remove his padlock and get the contents of the briefcase.

Discuss the security of this scheme. Are there any ways in which an attacker can disrupt this communication? How can Alice and Bob make the scheme more secure? [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: $p=17, g=3, a=7, y_a=3^7 \bmod 17=11, k_a=4$

Bob : $p=17, g=3, b=10, y_b=3^{10} \bmod 17=8, k_b=5$

The following table shows inverses mod 17 which you may need to help you with your answer. [10]

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

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

b) How can Bob use his RSA keys to digitally sign a message for Alice? How does Alice confirm that the signature is genuine? [4]

c) Alice has public and private RSA keys (n=85, e=7) and (d=55).
Bob has public and private RSA keys (n=77, e=17) and (d=53).

Assuming the role of Bob, and showing all your working, encrypt **and** sign the message m=19 to send to Alice. [8]

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

e) Re-write your answer to part b) showing how a hash function may be used in conjunction with RSA to produce a digital signature. [3]

f) What are the advantages of using the scheme of part e) rather than the scheme of part (b) when producing a digital signature? [2]

5. a) PGP combines public and symmetric key cryptography to provide confidentiality as follows:

- Alice creates a message m and a random session key k.
- Alice encrypts the session key using Bob's public key and a public key cryptosystem to obtain k'.
- Alice encrypts the message m using a symmetric cryptosystem with the session key k to obtain ciphertext c.
- Alice sends Bob the values of k' and c.

i. List the steps that Bob must take in order to recover the message. [4]

ii. What changes must Alice make to the scheme above if she wishes to compress the message as well as provide confidentiality? [2]

iii. Name three other services that PGP provides. [3]

b) PGP uses a *web of trust* to enable users to decide whether or not to trust that a public key is genuine. Other protocols make use of *certificates*. Give one advantage and one disadvantage of using certificates. [2]

c) 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]

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