UNIVERSITY OF LONDON 291 0326E

FOR EXTERNAL STUDENTS - EASTERN

B.Sc. EXAMINATION 2005

COMPUTING AND INFORMATION SYSTEMS

CIS326 Computer Security

Duration: 2 hours 15 minutes

Date and time: Tuesday, 24 May 2005 : 2.30 - 4.45 pm

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.

UL05/489

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

1. a) Name and briefly explain six features that should be provided by a good security system. [6]

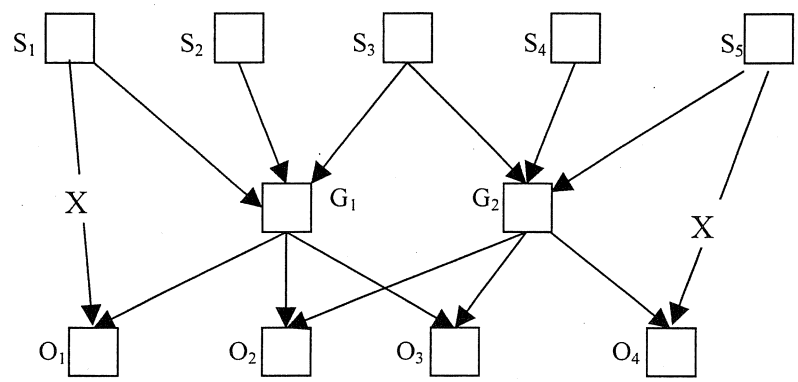
b) A multi-user distributed system provides *subjects* access to *objects* to perform *operations*. Give two examples of a subject and two examples of an object. [2]

c) Copy and complete the following table, which shows the relationship between operations and access modes. [2]

	Read	Write	Append	Execute	Delete
Observe	√				
Alter					

d) Give an example of **a situation** where a subject may have permission to alter an object without observing it. [1]

e) Consider the following graph which expresses group membership and access control:



Represent the access rights expressed in the graph above as an ***access control list*** according to subject. [5]

f) A password system is used to prevent unauthorized access to a computer system. Give four measures that can be taken by the user, and four measures that can be taken by the system, in order to prevent or detect a security breach. [4]

g) i) A password in a particular system can be made up of any of 50 different keyboard characters. What is the size of the keyspace for this system if passwords are 4 characters long? [1]

ii) The same system requires users to change their passwords once every three months, and insists on a minimum password length of n characters. Assuming that an automated password cracker can check 10,000 passwords per minute, what is the least possible value of n that can be used in order to prevent a successful exhaustive search attack? [4]

2. A commercially available symmetric key cryptosystem, called XYZ, has blocks of size b bits and keys of size k bits.

a) Why does the value of k need to be large? With modern algorithms what would you estimate to be the smallest value of k that could guarantee security? [2]

b) How could XYZ be modified to a new symmetric key cryptosystem called double-XYZ, so that the blocksize is still b but the keysize is $2k$. Explain the suggested encryption and decryption algorithms for double-XYZ. [6]

c) State whether each of the following statements is true or false and justify your answers: [6]

i) It takes twice as long to encrypt using double-XYZ as it does using XYZ.
ii) It takes twice as long to transmit a block of ciphertext using double-XYZ as it does using XYZ.
iii) It takes a cryptanalyst twice as long to do an exhaustive key search for double-XYZ as it does for XYZ.

d) If Alice and Bob are using a symmetric key cryptosystem to communicate, they will both need to know the key. Describe three different methods that Alice could use to securely exchange a key with Bob. [11]

3. a) Describe the El Gamel public key cryptosystem. Your answer should include [10]

i. The generation of public and private keys
ii. The encryption algorithm
iii. The decryption algorithm
iv. A justification for the security of the algorithm

b) Bob has private El Gamel key ($p=23$, $g=5$, $a=6$). What is the value of Bob's public key? [2]

c) Alice has encrypted a message using Bob's public key. The ciphertext that Alice sends to Bob is $(r=4, c=7)$. Showing all your working, use Bob's private key to recover the message. [4]

d) Describe the algorithm for fast modular exponentiation, that is the computation of $x^n \bmod m$. Your answer may be in pseudocode if you wish. [3]

e) Show that the algorithm described in part d) above is of complexity $O(b^3)$ where b is the size of the parameters x, n and m. [2]

f) Hence show that although the El Gamel algorithms for encryption and decryption are different, they both take approximately the same amount of time to execute. [4]

4. a) Suppose that a mathematician found a method that could be used to factorise a large composite number efficiently. Given a composite number n the method could quickly find p and q such that $p*q = n$. Explain why the security of the RSA public key cryptosystem would be compromised. [4]

b) Bob has a public RSA key $(n = 221, e = 5)$. He sends Alice a message m and the digital signature s of the message. Bob calculates the signature by computing $s = m^d \bmod n$ where d is Bob's private key. The message that Alice receives is $(m = 91, s = 72)$. Should Alice accept the message as genuine or not? You must give a justification for your answer. [8]

c) Name the four properties that a cryptographic hash function should possess and explain why each of these is important. [6]

d) Give a brief description of SHA-1, the Secure Hash Algorithm. [4]

e) What is the advantage of using a hash function when producing a digital signature? [3]

5. Pretty Good Privacy (PGP) provides security for electronic mail systems.

a) Describe how PGP provides simultaneously confidentiality, authentication and compression. [14]

Your answer should describe how a user compresses, digitally signs and encrypts a message and how the receiver determines the original message and proves that it is genuine. It is not necessary to give specific details about particular hash functions, symmetric cryptosystems or public key cryptosystems, but you should indicate what protocols you are assuming are available to each of the participants.

b) Name two advantages that the compression stage brings to PGP. [2]

c) Explain why there is sometimes a difficulty in sending encrypted text by electronic mail and describe how PGP overcomes this difficulty. [6]

d) Why does PGP allow users to have more than one set of public/private keys? How is this use of multiple keys managed? [3]

END OF EXAMINATION