UNIVERSITY OF LONDON
GOLDSMITHS COLLEGE

B.Sc. Examination 2003
Western Zone

Computing and Information Systems
Computer Science

IS53012A Computer Security

Duration: 2 hours 15 minutes

*Answer **all questions** in section A (48 marks) and **two questions** (26 marks each) from section B.*

Electronic calculators may be used. The make and the model should be specified on the script. The calculator must not be programmed prior to the examination. Calculators which display graphics, text or algebraic equations are not allowed.

This examination paper must not be removed from the examination room.

Section A

You must answer all 8 questions in this section. There are 6 marks for each question.

1. Discuss how an *access control table* is used to permit a subject to perform an operation on an object. [3]

   Write down the table for the following requirements:

   There are two users A and B and 3 files f, g, h. The user A has read and write access to f, g and has execute access to h. The user B has write access to g, h. [1]

   Give an example of an operation where the subject can alter an object but not observe it. [1]

   What are the disadvantages of access control tables? [1]

2. Give an account of how a directed graph, which has vertices as security labels, can be used for access control. [3]

   A department has two secure sections, *personnel* and *resources*. Documents in the department are either concerned with personnel, with resources, with both or with neither and the security labels are respectively $\{p\}, \{r\}, \{p, r\}$ or $\{\}$. Draw the directed graph for the security policy. [1]

   What security label would be assigned to the head of department? What security label would be assigned to the deputy head of resources? What security label would be assigned to a document concerned exclusively with personnel? [1]

   Decide using your graph and your answers whether or not the deputy head of resources would have access to the document concerned exclusively with personnel. [1]

3. In a cryptosystem why is a large keyspace and a large blocksize essential for security? [1]

   What are the blocksize and keysize for the *Data Encryption Standard (DES)*? [1]

   Why is DES now considered to be weak? [1]

   Describe *Triple-DES* in terms of DES. [2]

   What are the blocksize and keysize for Triple-DES? [1]

4. Name the 4 properties that a cryptographic hash function should possess. [2]

   Give a brief overview of the *Secure Hash Algorithm, SHA-1.* [3]

   How certain are we that SHA-1 has the 4 required properties of a cryptographic hash function? [1]

5. The public key cryptosystem, *RSA*, has a public key consisting of two numbers n, e and a private key, d. What is the relationship between e, d and n? [1]

   A message m is a number satisfying $0 \leq m < n$ and its corresponding ciphertext is c. What is c in terms of m, e, n? What is m in terms of c, d, n? [1]

   Why is RSA considered secure? [1]

   Explain how the RSA scheme can be used to *digitally sign* a message. [2]

   Why does the receiver accept the signature as genuine? [1]

6. The Needham-Schroeder protocol is a method for exchanging a session key between two users A and B using a trusted third party S. Denote by K_{AS} the symmetric key between A and S. Denote by K_{BS} the symmetric key between B and S.

   In the protocol, what does A initially send to S? [1]

   What does S then send to A? [2]

   What does A next send to B? [1]

   In this protocol, why is it not possible for another person C to masquerade as A? [2]

7. Describe the *X.509* protocol for the certification of identities and public key cryptographic keys. [6]

8. The t of n protocol is used for key escrow. In this protocol, it is required to divide a key into n pieces to give to n individuals, so that any set of t individuals can use their t pieces to determine the original key but no set of $(t-1)$ individuals can determine the key or obtain any information which makes the determination of the key easier.

   Describe a protocol for the case $n = 2$ and $t = 2$. [2]

   Describe a protocol for the case $n = 3$ and $t = 3$. [2]

   Show that the protocol for the case $n = 2$ and $t = 2$ has the desired properties. [2]

Section B

Answer two questions from this section. There are 26 marks for each question.

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

   Describe the following threats to the process:

   (a) password guessing; [2]

   (b) password spoofing; [2]

   (c) reading the password file. [2]

   Explain defences that the system can employ and defences that the user can employ to reduce the threat of password guessing. [5]

   Define what is meant by a *one-way function*. [2]

   Describe their use in cryptographically protecting the password file. [3]

   A hacker obtains access to a password file which has been cryptographically protected. Describe how the attacker may do an exhaustive search to determine the password of a particular user. [2]

   What two major factors affect the time it takes for this attack? [2]

   For each factor, describe how the system can ensure that the attack takes too long to be effective. [4]

2. State the *discrete logarithm problem* for modular arithmetic. [2]

   Describe how it is used in the *El Gamal* public key cryptosystem. Your description should include the generation of the keys, the encryption algorithm, the decryption algorithm and justification for the security. [12]

   What are the advantages and disadvantages of the El Gamal public key cryptosystem when compared with the RSA public key cryptosystem? [4]

   Describe how the discrete logarithm problem is used in the *Diffie-Hellman key exchange protocol.* [3]

   Comment on the security of the Diffie-Hellman protocol. [2]

   Showing all your working, illustrate the Diffie-Hellman protocol by determining the key in the case where the prime $p = 11$, the generator $g = 2$, and the two random numbers generated by the two parties are $a = 3$ and $b = 4$. [3]

3. Why is the study of the *computational complexity* of certain algorithms essential to the study of cryptography? [2]

   What is meant by the *size* of a positive number n? [1]

   What does it mean to say that the time required to add two large numbers of size b is $O(b)$? [1]

   For each of the following problems, *state* the computational complexity of the standard algorithm:

   (a) multiplying two numbers of size b; [1]

   (b) dividing a number of size $2b$ by a number of size b. [1]

   For each of the following problems, *determine and justify* the computational complexity of the appropriate algorithm:

   (a) given x, y, m with $0 \leq x, y < m$, computing $(xy) \bmod m$; [2]

   (b) given a, b, c, m with $0 \leq a, b, c < m$, computing $(abc) \bmod m$. [2]

   Describe the algorithm for modular arithmetic exponentiation for computing $x^n \bmod m$, where $0 \leq x, n < m$, which is based on the binary representation for n. [6]

   If m has size b, show that the algorithm has computational complexity $O(b^3)$. [4]

   Showing all your working, illustrate the algorithm by computing $2^{10} \bmod 13$. [3]

   The average time for the modular arithmetic exponentiation algorithm when $b = 100$ is 0.001 seconds. What is the average time when $b = 200$? [3]

4. Pretty Good Privacy (PGP) provides security for electronic mail systems. Describe how PGP provides *confidentiality and authentication*. Your answer should indicate how a sender digitally signs and encrypts a message and how the receiver determines the message and authenticates. Specific details about particular hash functions, symmetric cryptosystems and public key cryptosystems should not be given. [12]

   Indicate the changes to the scheme if the sender also wishes to *compress* a message as well as provide *authentication and confidentiality*. [5]

   In the last scheme, why is the message encrypted after compression rather than compression applied to the ciphertext? [2]

   Explain how PGP overcomes the problem that some electronic mail systems only allow blocks of ASCII text to be sent? [7]