UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

B.Sc. Examination 2002

Computing and Information Systems

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. The following six features should be provided by a security system. For each, write a sentence describing what is meant by the feature. [6]

   (a) integrity,

   (b) availability,

   (c) non-repudiation,

   (d) authentication,

   (e) accountability,

   (f) access control

2. Describe briefly the threat to the process of identification called password guessing. [2] Name and describe briefly two ways that a system can counter password guessing. [2] Name and describe briefly two ways that a user can counter password guessing. [2]

3. DES is the abbreviation for the Data Encryption Standard. What is the blocksize and keysize for DES? [2]

   Describe Triple-DES, stating clearly the blocksize, keysize, how a message is encrypted, how ciphertext is decrypted. [4]

4. What is the computational complexity of modular multiplication, that is determining $(x*y) \bmod m$ where x, y, m all have size b? [2]. In a particular implementation, it takes $10\mu s$ to perform a modular multiplication when $b = 50$. How long will it take, approximately, when $b = 200$? [2]

   For one of the following problems there is no known computationally efficient algorithm when b is large (for example $b = 600$). Which is it, giving a brief explanation? [2]

   (a) modular addition: computing $y = (x + z) \bmod m$ where x, z, m are given and all have size b,

   (b) modular exponentiation: computing $y = g^k \bmod m$ where g, k, m are given and all have size b,

   (c) factorising a number n of size b,

   (d) solving the modular equation for x: $y = (a*x) \bmod m$ where a, y, m are given and all have size b.

5. What is the computational complexity of the fast exponentiation algorithm for modular arithmetic? [2] Using the fast exponentiation algorithm and showing all your working, compute the value of $5^{14} \bmod 17$. [4]

6. What is the discrete logarithm problem for modular arithmetic? [2] Name and describe a key exchange protocol based on the problem. [4]

7. Pretty Good Privacy (PGP) provides security for electronic mail systems. One service it offers is e-mail compatibility. Name the other 4 services that PGP offers [2]. What is Radix-64 and how does it help to enable e-mail compatibility? [4]

8. What is meant by key escrow? [1] Describe a protocol where 3 individuals have pieces of a key k. No one individual has any information which makes the determination of the key k easier. However any two of them can work together to determine k completely. [5]

Section B

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

1. Give an account of the possible structures used for access control. [14] Your answer should include, but not necessarily be limited to, definitions and use of the following structures:

   (a) tables,

   (b) lists,

   (c) groups,

   (d) protection rings,

   (e) graphs.

   What two properties make a graph access control a lattice? [2] An organisation has two sections finance and personnel. Staff belong to none, one or both sections. Documents are either classified as secret or non-confidential. Security levels are represented by a pair (X, Y) where X is either secret or non-confidential and Y is a subset of the set $\{finance, personnel\}$. How many security levels are there? [1] Define the rule for determining if one security level (X_1, Y_1) dominates another (X_2, Y_2). [3] Draw the lattice of security levels. [6]

2. (a) A cryptanalyst can attack a symmetric key cryptosystem. One type of attack is called the known message attack. Name and describe in one sentence three other types of attack. [6]

(b) In a known message attack on a symmetric key cryptosystem, one strategy for a cryptanalyst is to try all possible keys. Describe a strategy for one of the types of attack that you answered in part (a). [4]

(c) A symmetric key cryptosystem should have a large alphabet and a large keyspace. Explain why each of these properties is important.[4]

(d) For symmetric key cryptosystems, there are issues relating to key management. Describe these issues and some possible solutions, commenting on the suitability or otherwise of each solution. [12]

3. (a) Describe the RSA public key cryptosystem. [13] Your answer should include, but is not limited to, the following:

   i. generalisation of Fermat's theorem to the case where the modulus is a product of two primes,

   ii. generation of private and public keys

   iii. the encryption algorithm

   iv. the decryption algorithm

   v. the basis for the security of RSA

   (b) Name four essential properties of a cryptographic hash function used for digital signatures (for example SHA-1), explaining for each property why it is essential. [6]

   (c) Explain how RSA and SHA-1 can be used to provide an efficient digital signature. [7]

4. Describe the Needham-Schroeder protocol for exchanging a session key between two subjects which uses symmetric key cryptosystems and a trusted third party. [12]

   Alice wishes to send Bob a message and uses the Needham-Schroeder protocol to generate a session key. Charles is a cryptanalyst who has access to communication traffic between any two of Alice, the trusted third party and Bob. How does the protocol overcome the following problems:

   (a) Charles determining the session key [2]

   (b) Charles masquerading as Alice [3]

   (c) Charles masquerading as Bob [3]

   (d) Charles preventing Bob from receiving any information from Alice [3]

   (e) Charles replaying a previous key generation. [3]