2910326 Computer security

Examination paper: Zone B

Time allowed: two hours and fifteen minutes

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.

A hand held calculator may be used when answering questions on this paper but it must not be pre-programmed or able to display graphics, text or algebraic equations. The make and type of machine must be stated clearly on the front cover of the answer book.

1. (a) After reading a newspaper "scare story" about password security, Walter has decided to implement strict rules regarding the passwords used by the staff in his company. Walter insists that:

   - Staff passwords are of length 15 characters or more.
   - Staff change their passwords at least once at week.
   - Every password contains a mix of letters and digits.

   i. Explain why Walters password policy is likely to make the password system at his company less rather than more secure.

   [3]

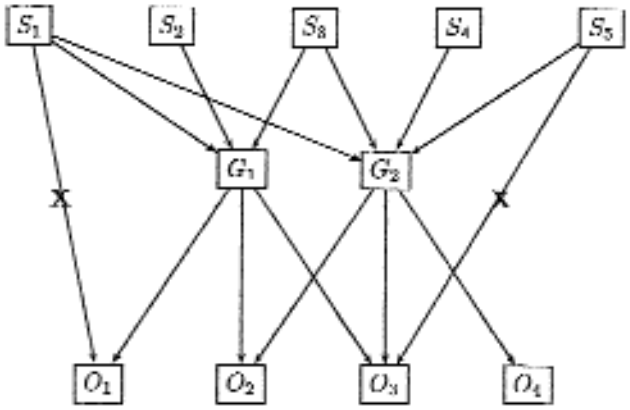
   ii. Write a more suitable password policy explaining the importance of each rule you suggest.

   [10]

   iii. Assuming that a password cracking program can check 10,000 passwords per minute, calculate the average amount of time that it would take to find a password based on the policy you have written in part [ii].

   [4]

   (b) The graph below shows the group membership and access rights of five subjects.



   i. Determine the access rights of each subject expressing them in the form of an access control list.

   [5]

   ii. Is the graph shown a lattice? Explain your answer.

   [3]

2. (a) Alice is using a symmetric key cryptosystem to transmit private communications.

   i. Name two commercially available symmetric key cryptosystems.

   [2]

   ii. How many different keys does Alice require in order to communicate with eleven other people using the symmetric key cryptosystem?

   [1]

   iii. Assuming that Alice and the eleven other users all communicate with each other, how many different keys are needed in total?

   [2]

   iv. Describe how the Needham-Schroeder protocol could be used to exchange keys between Alice and another user of the symmetric key cryptosystem.

   [8]

   (b) The master password of a company can be used in an emergency to access the password file of the company security system.

   i. There are three company directors. Describe how the directors could use a 3 of 3 key escrow protocol to protect the master password from abuse.

   [5]

   ii. Suggest why a 3 of 3 key escrow protocol might be impractical.

   [1]

   iii. Suppose the three directors instead use a 2 of 3 key escrow protocol and that the directors hold the following keys:

   $$\begin{aligned} &\text{Director 1}: (x_1 = 5\ , k_1 = 4\ , p = 43) \\ &\text{Director 2}: (x_2 = 39, k_2 = 12, p = 43) \\ &\text{Director 3}: (x_3 = 27, k_3 = 37, p = 43) \end{aligned}$$

   Given that $(34 * 19) = 1 \bmod 43$ show how Director 1 and Director 2 can work together to find the master password.

   [6]

3. (a) i. Describe the fast algorithm for modular exponentiation, that is, the computation of $x^n \bmod m$. Your answer may be given as psuedocode if you wish.

[6]

ii. Show that the algorithm requires $b(n)$ multiplication steps where $b(n)$ is the size of the number n. Hence, assuming that each multiplication step has a computational complexity of $O(b^2(n))$, derive the computational complexity of the fast algorithm for modular exponentiation.

[4]

(b) i. Describe the key generation, encryption and decryption protocols for the RSA public key cryptosystem.

[10]

ii. Showing all your working, decrypt the ciphertext block $c = 526$ using RSA keys ($e = 463, d \quad 7, n = 703$).

[5]

4. (a) State the discrete logarithm problem.

[2]

(b) Using the numbers $g = 2, p = 67, a = 13, b - 7$ show how the Diffie Hellman key exchange protocol makes use of the discrete logarithm problem to enable Alice and Bob to share a secret key.

[6]

(c) Explain why the Diffie Hellman key exchange protocol is vulnerable to a man-in-the-middle attack.

[6]

(d) Name a public key cryptosystem which uses the discrete logarithm problem as the basis for its security and describe its key generation protocol.

[5]

(c) If Alice wants to send Bob an encrypted message, she will look up his public key in a directory. Describe the X.509 certification protocol and how it can be used to prevent an attacker putting their own key in the directory in the place of Bob's key.

[6]

5. (a) The following are seven features that may be provided by a security system. For each write a sentence describing what is meant by the feature.

   i. confidentiality
   ii. integrity
   iii. availability
   iv. non-repudiation
   v. authentication
   vi. access control
   vii. accountability

   [7]

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

   i. Describe the PGP protocol for exchanging an encrypted, signed message.

   [7]

   ii. Which of the security features listed in part a) are provided by the PGP protocol?

   [5]

   iii. Describe how PGP overcomes problems particularly associated with email security by using radix-64 conversion and segmentation.

   [6]