Student ID ……

AK3697 Bachelor of Computer and Information Sciences (BCIS)

FINAL EXAMINATION -- SAMPLE

xxxxx

PAPER DESCRIPTION: Information Security Technologies

PAPER CODE: COMP607

TIME ALLOWED: 3 hour exam + 10 minutes reading time

TOTAL MARKS: 100

INSTRUCTIONS:

1. Answer ALL the questions.
2. Write your student ID clearly on every page.
3. Write your answers in the spaces provided. If you need additional space, use the blank pages provided at the back. Make sure you write the question number clearly.
4. Hand in this question paper at the end of the examination.
5. This is a closed-book exam. No notes, books, or any references.
6. Only non-programmable calculators are allowed.
7. Keep away all other electronic devices including phones, etc.
8. Paper dictionaries are permitted.
9. Correction fluid is not permitted.

ADDITIONAL MATERIALS: NONE

Part I

Question 1 [10 marks]

a) Use the Caesar's cipher with key=4 and encrypt the following plaintext message. [3 marks]

WASTE NOT WANT NOT

b) State what is meant by a mono-alphabetic substitution cipher. Explain how the mono-alphabetic cipher can be broken if enough cipher text encrypted using the same key is available to the attacker. [3 marks]

c). Explain how an attacker can break any cipher using the "brute force" attack. [2 marks]

Question 2 [10 marks]

(a) The DES algorithm is known to be quite robust against known analytically attacks, but it has a very serious weakness. Explain what is this weakness. In spite of this, the DES algorithm can be used to provide very strong encryption. Explain with the help of a diagram or mathematical expressions, how the DES algorithm can be used in a secure way using 2 keys, K_{s1}, and K_{s2}, each of 56 bits. [5 marks]

(b) Explain why encryption algorithms such as DES and AES are called symmetric key algorithms. [3 marks]

(c) Explain the main difference in the way a block cipher and stream cipher works. [2 marks]

Question 3 [10 marks]

(a) An administrator uploads a file to a server for users to download over the Internet.

(i) What else should the administrator provide so that the users can check whether the file downloaded on their computers is exactly same as the file on the server, i.e. there is no error whatsoever? [3 marks]

(ii) What should the user do to check the integrity of the downloaded file? [3 marks]

(b) Explain how servers store usernames and their passwords in such a way the even if two different users have the same password, their stored passwords are different. [4 marks]

Question 4 [10 marks]

(a) Explain how *Alice* and *Bob* can use the DH algorithm to establish a shared secret key. Consider that they use the global parameters: generator $G=3$ and prime number $n = 7$.
Show what each party computes, the values they exchanged, and the shared key. [4 marks]

(b) The DH algorithm is secure even though an eavesdropper can view all the messages exchanged between the two parties. Explain the main requirements for the DH algorithm to be secure. [3 marks]

(c) The DH algorithm can also be implemented using elliptic curves (ECDH). What is the main benefit of elliptic curver implementation compared to the normal DH algorithm. [3 marks]

Question 5 [10 marks]

(a) *Bob* wish to encrypt a message *M* and send it to *Alice* over an insecure channel such as the Internet. They use the RSA algorithm. *Alice* has public key <*e*,*n*> and private key <*d*,*n*>. Explain the steps and computations required for *Bob* to encrypt the message *M* for *Alice*. [5 marks]

b) Alice wishes to compute her RSA public and private keys. She chooses primes p = 3, q = 11. If her public key exponent is e=3, show how she would calculate her private key exponent d. [5 marks]

Part II

Question 6 [10 marks]

(a) State the five fundamental security principles in "DOLLS" and explain each one with an example. [5 marks]

(b) Explain what is meant by phishing attack and how this can be carried out. [3 marks]

(c) Briefly describe the main features of these three main types of malware: worms, viruses, and trojans.

[2 marks}

Question 7 [10 marks]

(a) Explain these terms: hot site, warm site, and cold site, in the context of business continuity. [6 marks]

(b) Explain how storage redundancy can be achieved in a server using RAID level 1 (mirroring) and RAID level 5 (independant disks with distributed parity). [4 marks]

Question 8 [10 marks]

(a) What are the three mechanisms commonly used for authentication in computer and information systems? [3 marks]

(b) If a user enters his/her username and password to access a website, which of the authentication mechanism being used? State two security risks for this method of authentication. [3 marks]

(c). What is multi-factor authentication? Explain using an example of two-factor authentication that is in use today. [4 marks]

Question 9 [10 marks]

(a) Explain the meaning of each component of AAA in the context of information and computer security. [6 marks]

(b) State the main purpose of a Key Distribution Center (KDC) in a network which has a large number of users and servers. [2 marks]

(c) What is the role of a RADIUS server in a network? [2 marks]

Question 10 [10 marks]

(a). What are the two main methods of authenticating users when connecting to a secure wireless network? State, with reason, which one is prefered for home networks and which one is prefered for enterprise networks. [6 marks]

(b) Messages between a wireless device and access point must be encrypted. One method for encryption available for older devices is WEP. What is main weakness of WEP? [2 marks]
Which is the current encryption method that is commonly used today in wireless network access points? [2 marks]

END