KABARAK UNIVERSITY

UNIVERSITY EXAMINATIONS
2010/2011 ACADEMIC YEAR

FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE

COURSE CODE: BMIT 416

COURSE TITLE: INFORMATION TECHNOLOGY SECURITY, AUDIT AND ETHICS

STREAM: Y4S1

DAY: FRIDAY

TIME: 9.00 – 11.00 P.M

DATE: 10/12/2010

INSTRUCTIONS:

- **Section A answer *ALL* questions in this section**

PLEASE TURN OVER

QUESTION ONE (40 MARKS)

a)

i). Distinguish between the terms Authentication, authorization and accounting as applied in computer security **[6 marks]**

ii). Outline the FOUR factors on which Authenticators are commonly based. **[4 marks]**

b)

i). When thinking about security, it is helpful to think in terms of *assets, threats, vulnerabilities,* and *attacks* outline the meaning of each of these terms giving relevant examples. **[6 marks]**

ii). The IT department for Widget Warehouse has a general understanding of security but they are very in experienced with the various attacks an intruder can use to exploit their network resources. Create a list of SEVEN attacks intruders can use maliciously against the Widget Warehouse network and provide a brief description of each. **[7 marks]**

c)

i). State THREE basic types of access controls that provide different levels of protection to the files in a computer system. **[3 marks]**

ii). Consider data that is stored over time in a mandatory access control based system. Will the contents of files containing highly classified ("top secret") information be necessarily more trustworthy than material stored in files marked unclassified? Justify your answer **[3 marks]**

d)

i). Outline the objective of the need to know principle **[2 marks]**

ii). Explain the principle of list privileges as applied in information security **[3 marks]**

iii). Outline Benefits of principal of lease privileges **[6 marks]**

SECTION B ANSWER *ANY THREE* QUESTIONS IN THIS SECTION

QUESTION TWO (20 MARKS)

a) Distinguish between

i). Cryptography and steganography **[4 marks]**

ii). Logging and Auditing **[4 marks]**

b)

i). What is a cryptographic hash function? **[3 marks]**

ii). The ideal cryptographic hash function has FOUR main or significant properties Outline these properties **[4 marks]**

iii). Cryptographic hash functions have many information security applications outline any FIVE of these uses **[5 marks]**

QUESTION THREE (20 MARKS)

a)

i). "Access control matrices can represent anything that is represented by access control lists." State whether this statement is true or false and justify your answer: **[3 marks]**

ii). The management of XYZ Company has asked the network administrator to recommend software to achieve two objectives:

a) detect Trojan horse malware and prevent it from affecting desktop computers, and

b) detect and prevent reconnaissance attacks such as port scanning and ping sweeps After careful consideration, the network administrator recommends Norton Anti- Virus Corporate Edition. Is this solution sufficient? Why or why not **[2 marks]**

b)

i). Explain the terms "proof of submission" and "non-repudiation" in an electronic mail system **[2 marks]**

ii). Describe the use of a digital signature for origin authentication **[3 marks]** c)

i). Outline THREE characteristics of Caesar cipher that makes a brute force cryptanalysis easy to perform **[3 marks]**

ii). Explain the meaning of totient n or $\varphi(n)$of a positive integer n as applied in number theory. Hence compute $\varphi(9)$ **[4 marks]**

iii). Suppose Alice chooses $n = 35$ as her RSA modulus, and chooses $e_A = 7$ as her public exponent. Hence her public key is (n, e_A). Calculate her private decryption exponent d_A. **[3 marks]**

QUESTION FOUR (20 MARKS)

a) Consider the following confidentiality classification with the security levels from the most sensitive at the top and the least sensitive at the bottom and the associated categorization of users and documents grouped by their security clearances.

Confidentiality classification	***User categorization by security clearances***	***Document categorization by security clearances***
TOP SECRET	Tamara	Personal Files
|	|	|
SECRET	Sally	Electronic Mail Files
|	|	|
CONFIDENTIAL	Claire	Activity Log Files
|	|	|
UNCLASSIFIED	Ursula	Telephone List Files

i. Sate the rule used by the confidentiality model to assign file read privileges to users **[2 marks]**

ii. Explain the documents read privileges of Tamara and Claire assuming that the discretionary access control allows it. **[2 marks]**

iii. Supposing the star property rule (no writing down rule) does not apply and Tamara decides to write personal files content into the activity log files. Explain how this would affect secrecy assuming that discretionary access control is set appropriately. **[2 marks]**

iv. State the tranquility rule and explain its importance with respect to security **[2 marks]** b)

i). What is ARP spoofing **[2 marks]**

ii). Outline any FOUR symptoms of ARP spoofing **[2 marks]**

c)

i). State Kerckhoff's principle. Explain briefly why a cryptosystem designed by someone who follows this principle is likely to be stronger than one designed by someone who does not. **[4 marks]**

ii). Explain the main drawback of the onetime pad cryptosystem? **[4 marks]**

QUESTION FIVE (20 MARKS)

a) Distinguish between the terms '*Security model', ' security policy' and 'security mechanism'* as applied in computer security **[5 marks]**

b) Identify at least TWO security components that make up each of the following security solutions **[6 marks]**

i). Trust and identity

ii). Secure Connectivity

iii). Threat Defense

b) Study the following password encryption program written in C++; hence answer the questions that follow

```
#include <iostream>
#include <string.h>
using namespace std;

int main()
{

  char str1[80];
  int i = 0;
  int offset;

        cout << "please enter your password\n";
        cin >> str1;
        cout << "What do you want your offset number to be?\n";
        cin >> offset;
        while(i<strlen(str1)){
           str1[i] = (int(str1[i]) + offset)%26;
           i++;
        }

        cout << str1<<endl;
        return 0;
}
```

i). State the cipher algorithm implemented by this program **[1 mark]**

ii). Suppose the user enters the value 5 for the offset number, what would the password MAKASI encrypt to? Show your working **[4 marks]**

c)

i. Define the term ‘zombie’ with respect to malicious software **[2 marks]**

ii. Explain how zombies can be used by business competitors to gain business mileage **[2 marks]**