INSTITUTE OF TECHNOLOGY
BLANCHARDSTOWN

Year	Year 1
Semester	Semester 1 Repeat
Date of Examination	Friday 23rd August 2013
Time of Examination	1.00pm – 3.00pm

Prog Code	BN518	**Prog Title**	Master of Science in Computing	**Module Code**	MSIT H6020

Module Title	Secure Communications and Cryptography

Internal Examiner(s): *Mr Mark Cummins, Mr Mark Lane*
External Examiner(s): *Mr Michael Barrett,*
Dr Tom Lunney

Instructions to candidates:

1) **To ensure that you take the correct examination, please check that the module and programme which you are following is listed in the tables above.**
2) **Question one in Section A is compulsory. Candidates should attempt all parts of question one and ANY other two questions from Section B.**
3) **This paper is worth 100 marks. Question 1 is worth 40 marks and all other questions are worth 30 marks each.**
4) **Answers to each question must start on a new page.**

DO NOT TURN OVER THIS PAGE UNTIL YOU ARE TOLD TO DO SO

Section A: Compulsory Question *(40 marks in total)*

Question 1: Attempt all parts of this question *(5 marks each)*

(a) Describe the *CIA Security model* and discuss an extra element which could be added to improve the model. In your answer describe how cryptography is used to implement each aim of the model.

(5 marks)

(b) Describe how a one-time-pad, when implemented correctly has the desirable property of *perfect secrecy*.

(5 marks)

(c) Describe the similarities and differences between *encoding* and *encryption*. Give examples of when each would be used.

(5 marks)

(d) Explain the importance and role played by Certificate Revocation Lists (CRL) as part of the PKI.

(5 marks)

(e) Describe some of the types of vulnerability that may be exploited against cryptographic hashing.

(5 marks)

(f) Compare and contrast symmetric and asymmetric encryption. Give examples of well-known symmetric and asymmetric ciphers.

(5 marks)

(g) Given the values below, what will be the value of the shared secret key generated by Alice and Bob, assuming that they are using the Diffie Hellman algorithm?

A random prime	: 11
A generator	: 3
Alice's random secret	: 4
Bob's random secret	: 5

(5 marks)

(h) i. List the four main properties of an ideal cryptographic hash function.

(3 marks)

ii. In relation to hash functions what are collisions?

(2 marks)

Section B: Answer ANY two questions

Question 2 (30 marks)

(a) Every time we access a webpage via our PC or smart phone we leak personal information about ourselves. Detail what type of information users typically reveal when they visit a webserver, and outline the steps and precautions a user could take to minimise the data they reveal to webservers they visit.

(12 marks)

(b) Describe the difference between *block ciphers* and *stream ciphers* in cryptography and give examples of each.

(8 marks)

(c) Describe in detail the function and operation of the Data Encryption Standard (DES).

(10 marks)

Question 3 (30 marks)

(a) Describe how some communications are vulnerable to man-in-the-middle attacks, and explain the effectiveness of the security countermeasures typically used to counter these threats.

(10 marks)

(b) Describe the characteristics of hashing that makes it useful for cryptography, and describe some common uses for hashes.

(10 marks)

(c) Describe the problems associated with cryptographic key management and how public key cryptography can help to overcome these issues.

(10 marks)

Question 4 (30 marks)

(a) Describe, in detail, the steps an attacker would follow to attack and break the WEP key on a private network. In your answer make reference to some of the commonly used tools used to launch such attacks.

(12 marks)

(b) Two security options commonly used by WLAN administrators include mac address filtering and disabling SSID broadcasts. Show the weakness in each of these security mechanisms by describing in detail how an attacker could easily bypass each of these two mechanisms.

(8 marks)

(c) Describe the six categories of threats to communications security. In your answer, describe how cryptographic countermeasures can be combined to secure against each these threats.

(10 marks)