INSTITUTE OF TECHNOLOGY

BLANCHARDSTOWN

Academic term	2013-14
Year of study	Year 1 (Masters)
Semester	REPEATS - SEMESTER ONE
Date of examination	Monday 18 August 2014
Time of examination	1:00pm – 3:00pm

Programme code	**Programme title**	**Module code**
BN518 - Full Time	Master of Science in Computing	MSIT H6020
BN518 - Part Time	Master of Science in Computing	MSIT H6020

Module Title	Secure Communications and Cryptography REPEAT EXAM

Internal Examiner(s)	Mr. Mark Cummins, Mr. Jim Bowen
External Examiner(s)	Dr. Tom Lunney, Mr. Michael Barrett

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 table above.**
2.	**Attempt ALL PARTS of Question 1 and any TWO other questions.**
3.	**This paper is worth 100 marks. Question 1 is worth 40 marks and all other questions are worth 30 marks each.**

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

Section A: Attempt ALL parts of this question

All parts are worth 5 marks each

Question 1: (40 marks)

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

(5 marks)

b) Briefly explain the operation of a Smurf attack.

(5 marks)

c) While WPA is a definite security improvement over WEP, the WPA security mechanisms are not as strong as one might expect from a cryptographic perspective. Why is WPA not cryptographically stronger?

(5 marks)

d) Describe the strict avalanche criterion and explain why it is a desirable property for a cryptographic hash function.

(5 marks)

e) Briefly outline the AES protocol.

(5 marks)

f) Explain Shannon's definition of 'perfect secrecy' for ciphers.

(5 marks)

g) Tempest and EMC problems share many features, but solving one does not necessarily mean solving the other. However, there are three main steps to eliminate EMC leakage that are also common to Tempest. List these three steps.

(5 marks)

h) 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)

Section B: Answer ANY 2 questions from this section

(All questions carry equal marks)

Question 2 (Wireless Security – 30 Marks)

a) Describe in detail the operation of the WEP wireless security protocol.

(12 marks)

b) Explain the operation of the WPA wireless security protocol.

(8 marks)

c) Outline the functions provided by a RADIUS server as part of the authentication process on a WLAN.

(6 marks)

d) Explain the operation of a captive portal and detail how it provides ease of use for end users trying to access a Wi-Fi network.

(4 marks)

Question 3 (Digital Hashing – 30 Marks)

a) Describe in detail the development of the Secure hash algorithm (SHA).

(12 marks)

b) Outline the history and timeline of attacks against the MD5 algorithm.

(12 marks)

c) A cryptographic hash function must be able to withstand all known types of cryptographic attack. List and briefly explain each of the three types of resistance properties that a cryptographic hash function should exhibit.

(6 marks)

Question 4 (VPNs – 30 Marks)

a) Explain, with the aid of a diagram, the process of tunneling as it relates to VPNs.

(5 marks)

b) Two tunneling protocols that may be used with VPNs are L2TP (Layer 2 tunneling protocol) and IP Sec (IP security protocol). Compare and contrast both of these tunneling protocols.

(6 marks)

c) Threats to secure VPN systems can be divided into three areas. List and briefly describe each of these three areas.

(9 marks)

d) 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.

(10 marks)