INSTITUTE OF TECHNOLOGY BLANCHARDSTOWN

Year	Year 1
Semester	Semester 1 – Repeat Exam
Date of Examination	Wed. 17th Aug. 2016
Time of Examination	1.00pm – 3.00pm

Prog Code	BN518	**Prog Title**	Master of Science in Computing Full & Part time	**Module Code**	MSIT H6020

Module Title	Secure Communications and Cryptography

Internal Examiner(s): Mr. Mark Cummins
Mr. Jason Flood

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) 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) 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.

(5 marks)

b) What are the 5 criteria that secure communication should meet?

(5 marks)

c) Describe in detail how an attacker would perform an ARP poisoning attack on a switched network to perform a MITM attack.

(5 marks)

d) Describe WPA2

(5 marks)

e) What does the IV attack or CBC IV attack exploit

(5 marks)

f) List 5 steps to take in order to secure an access point

(5 marks)

g) Describe with the aid of diagrams how a linear feedback shift register operates

(5 marks)

h) List 5 sources of entropy?

(5 marks)

Section B: Answer ANY 2 questions from this section

(All questions carry equal marks)

Question 2 (30 Marks)

a) List 4 802.11 standards and discuss the key differences in the standards you choose.

(8 marks)

b) Outline the properties and operation of the RSA asymmetric cipher.

(10 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)

e) One of the weaknesses of a one-time pad (OTP) is that the OTP is malleable. Explain the implications of this weakness.

(2 marks)

Question 3 (30 Marks)

a) Prove that the OTP satisfies the consistency equation

(4 marks)

b) Can a stream cipher have perfect secrecy? Explain your answer.

(6 marks)

c) What can be said about an injective hash function

(2 marks)

d) In probability theory the birthday problem or birthday paradox can be explained as what?

(6 marks)

e) Explain the practical implementation of the MD5 algorithm

(12 marks)

Question 4 (30 Marks)

a) Illustrate using a worked example how an attacker could perform a practical MITM attack against two parties attempting to use Diffie-Hellman key exchange.

(10 marks)

b) What is a rainbow table, and what is it used for?

(2 marks)

c) What is the difference between a Hash, A MAC and Signature

(6 marks)

d) 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.

(5 marks)

e) What is the purpose of a Security association List (SAL) as defined in IP Sec?

(5 marks)

f) What is the most widely used PKI standard

(2 marks)