INSTITUTE OF TECHNOLOGY

BLANCHARDSTOWN

Academic term	2013-14
Year of study	Year 1 (Masters)
Semester	SEMESTER ONE
Date of examination	Monday 13th January 2014
Time of examination	12.30pm – 2.30pm

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

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

(5 marks)

b) RFC 1827, IP encapsulating security payload (ESP), describes two methods for using encryption to guarantee the integrity and confidentiality of data sent via the Internet (or via a private IP network). These are 'Tunnel-mode' and 'Transport-mode'. Briefly compare and contrast both of these modes.

(5 marks)

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

(5 marks)

d) Many cryptographic protocols (i.e. DH and RSA) are based on currently infeasible mathematic problems, such as the discrete logarithm problem or the large number factorisation problem. What would be the effect, and what protocols would be effected, if a solution to either of these problems was discovered tomorrow?

(5 marks)

e) The term, 'tempest' was coined by the US government to identify the problem of compromising radiations. It is used as a standard of protection against electronic hardware electromagnetic radiation. List some of the countermeasures used to design and construct security equipment to overcome Tempest threats.

(5 marks)

f) Compare and contrast each of the 3 different wireless LAN security protocols commonly used to encrypt network traffic.

(5 marks)

g) Describe the use of rainbow-tables in attacking stored hashed passwords, and outline how a developer can securely store their critical data rendering these types of attack ineffective.

(5 marks)

h) In relation to hash functions what is second preimage resistance?

(5 marks)

Section B: Answer ANY 2 questions from this section

(All questions carry equal marks)

Question 2 (Internet Security – 30 Marks)

a) Briefly explain the operation of a Fraggle attack.

(6 marks)

b) The launch of web browsers in the early 1990's caused a rush to develop secure protocols for use over the internet. Detail the development and timeline of the main internet security protocols during this period.

(8 marks)

c) Explain, in detail, the operation of the SSL/TLS protocol.

(8 marks)

d) Explain the various security issues and weaknesses relating to each of different SSL/TLS protocol versions.

(8 marks)

Question 3 (Asymmetric Encryption– 30 Marks)

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

(10 marks)

b) Explain the function of certificate authorities as part of a PKI, in your answer you should refer to certificate chains and X.509 certificates.

(10 marks)

c) 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)

Question 4 (Stream Ciphers – 30 Marks)

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

(6 marks)

b) A consequence of Shannon perfect secrecy theorem is that for a cipher to have perfect secrecy the key length must be >= to the message length. What are the practical implications of this?

(2 marks)

c) What is the consistency equation for ciphers?

(4 marks)

d) Outline how an attacker could perform a two-time pad attack against a security protocol that reuses keys within its one-time pad implementation.

(10 marks)

e) GSM, DVD encryption and Bluetooth all use the CSS protocol with a linear feedback shift register (LFSR). Cryptanalysis of CSS has resulted in the security for all of these systems being badly broken. Briefly outline the weaknesses in CSS that allowed these attacks.

(8 marks)