INSTITUTE OF TECHNOLOGY BLANCHARDSTOWN

Year	Year 1
Semester	Semester 1
Date of Examination	Mon 11th Jan 2016
Time of Examination	12.30pm – 2.30pm

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)

i. List **any three** weaknesses of the RC4 stream cipher.

(3 marks)

ii. List one modern security protocol that **incorrectly** uses RC4, resulting in the protocol being severely weakened.

(1 mark)

iii. List another modern security protocol that **correctly** uses RC4 within its implementation.

(1 mark)

b) Briefly outline at least 3 recent attacks against the SSL/TLS secure internet protocols used in the implementation of HTTPS.

(5 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.

(5 marks)

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

(5 marks)

e) 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)

f) 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)

g) 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)

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

(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.

(8 marks)

b) Explain the operation of the WPA wireless security protocol. **(7 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) Outline the functions provided by a RADIUS server as part of the authentication process on a WLAN.

(6 marks)

e) 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 (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)

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

(2 marks)

ii. Describe, with the use of a worked example, how an attacker might exploit the malleability of the OTP.

(8 marks)

iii. Prove that the OTP satisfies the consistency equation.

(4 marks)

iv. List any three real world examples of technologies that have used flawed implementations of a OTP resulting in possible two-time pad attacks.

(2 marks)

b) Describe in detail how you would break the DVD encryption algorithm CSS (Content Scrambling System).

(8 marks)

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

(6 marks)