INSTITUTE OF TECHNOLOGY BLANCHARDSTOWN

Year	Year 1
Semester	Semester 1
Date of Examination	Thurs 8th Jan 2015
Time of Examination	12.30pm – 2.30pm

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

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 <u>ALL PARTS</u> of Question 1 and any <u>TWO</u> 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)

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

(4 marks)

ii. How would you prevent this type of attack against Diffie-Hellman?

(1 marks)

d) Explain the key weaknesses in the design of the WEP protocol that make it vulnerable to attack.

(5 marks)

e) Given the parameters below, what would be the resulting ciphertext of RSA encrypting the message m.
Where m = 9, p = 11, q =13, e=7

(5 marks)

f) Many cryptographic protocols 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)

g) 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)

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

(5 marks)

Section B: Answer ANY 2 questions from this section

(All questions carry equal marks)

Question 2 (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)

Question 3 (Digital Signatures– 30 Marks)

a) What is the main purpose of digital signatures?

(2 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.

(8 marks)

c) Describe in detail the signing and verification process for digital signatures.

(8 marks)

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

(4 marks)

e) What is the purpose of each of the three elements of a digital signature algorithm?

(6 marks)

f) Which original algorithm is the basis for the current DSA?

(2 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)