INSTITUTE OF TECHNOLOGY BLANCHARDSTOWN

Year	Year 1
Semester	Semester 1 Repeat
Date of Examination	Thurs 20th Aug. 2015
Time of Examination	1.00pm – 3.00pm

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 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 a PKI.

(5 marks)

b) List and briefly explain the 4 classifications of cryptographic countermeasures used to ensure secure communications.

(5 marks)

c) If you are given a message (m) and its OTP encryption (c). Can you compute the OTP key from m and c? Explain your answer.

(5 marks)

d) 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)

e) As part of implementing the RSA algorithm, the values shown below were generated. What would be the resulting public and private keys in this example p = 11, d = 103, q =13, e=7

(5 marks)

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

(5 marks)

g) What is the purpose of a security association list (SAL) as defined in IPSec?

(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	: 7
A generator	: 5
Alice's random secret	: 4
Bob's random secret	: 3

(5 marks)

Section B: Answer ANY 2 questions from this section

(All questions carry equal marks)

Question 2: (Encryption - 30 marks)

a)

I. For what purpose is the Diffie-Hellman algorithm commonly implemented?

(2 marks)

II. Which of the CIA properties are present in the Diffie-Hellman algorithm?

(2 marks)

b)

I. What types of attack are possible against the default Diffie-Hellman algorithm?

(2 marks)

II. What additional mechanism is usually implemented with Diffie-Hellman to help avoid these attacks?

(2 marks)

III. Which of the CIA properties does this additional mechanism add to the Diffie-Hellman process?

(4 marks)

IV. Which of the CIA properties is never usually included as part of the process and why?

(2 marks)

c)

I. If Eve ,an eavesdropper, manages to capture the entire Diffie-Hellman exchange between two parties Alice and Bob, is it feasible for Eve to find the key, **K**, and why?

(4 marks)

II. What is the name given to this type of problem?

(2 marks)

d) Describe, with the aid of a diagram, the Diffie-Hellman exchange between two parties Alice and Bob, where Alice initiates the exchange.

(10 marks)

Question 3 (Stream Ciphers – 30 Marks)

a)

i. Briefly describe the operation of the Salsa20 stream cipher that forms part of the EStream project.

(4 marks)

ii. Can Salsa20 be used as a secure PRG? Explain why.

(2 marks)

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

(8 marks)

c) GSM, DVD encryption and Bluetooth all use linear feedback shift registers (LFSR) to perform hardware based stream ciphers. Cryptanalysis of LFSRs has resulted in the security for all of these systems being badly broken. Using any one of the technologies listed above as an example, briefly outline the weaknesses in LFSRs that have allowed these attacks.

(8 marks)

d)

i. Explain Shannon's definition of 'perfect secrecy' for ciphers.

(6 marks)

ii. 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)

Question 4 (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 the different SSL/TLS protocol versions.

(8 marks)