INSTITUTE OF TECHNOLOGY BLANCHARDSTOWN

Academic term	2016/2017
Year of study	5
Semester	SEMESTER ONE
Date of examination	Wed 11th Jan 2017
Time of examination	9.30am – 11.30am

Programme code	**Programme title**	**Module code**
BN528	Master of Science in Computing in Applied Cyber Security	MACS H6014

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 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) 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)

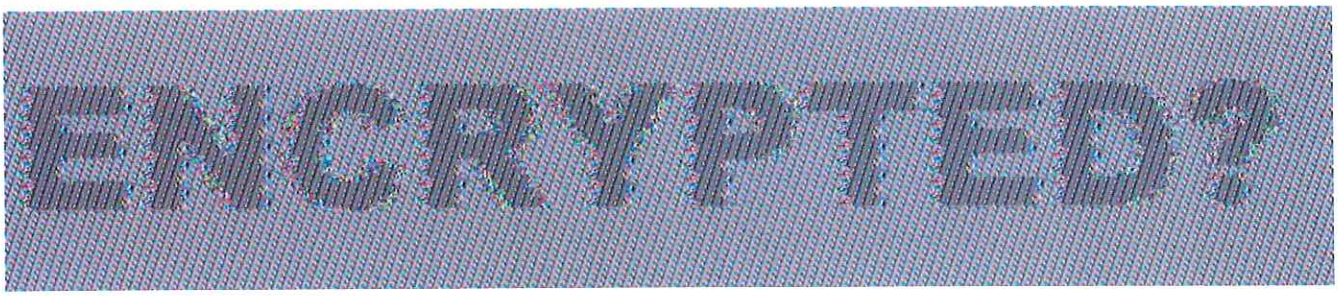
b) Briefly compare and contrast symmetric and asymmetric encryption.

(5 marks)

c) 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)

d) A recent audit and analysis of your companies encrypted image data, indicated a problem with the encryption, as the image data was still viewable even after encryption. What is the likely cause of the problem described and how should it be corrected.



(5 marks)

e) 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)

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

(5 marks)

g) Many cryptographic protocols are based on currently infeasible mathematic problems.

List the associated infeasible mathematic problems associated with

i. Diffie Helman **(1 mark)**

ii. RSA **(1 mark)**

iii. What would be the effect, if a solution to either of these problems was discovered tomorrow?

(3 marks)

h) Suppose you are told that the one time pad encryption of the message "attack at dawn" is *6c73d5240a948c86981bc294814d* (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key?

41	A
42	B
43	C
44	D
45	E
46	F
47	G
48	H
49	I

4A	J
4B	K
4C	L
4D	M
4E	N
4F	O
50	P
51	Q
52	R

53	S
54	T
55	U
56	V
57	W
58	X
59	Y
5A	Z
20	Space

(5 marks)

Section B: Answer ANY 2 questions from this section

(All questions carry equal marks)

Question 2 (Cryptographic Hashes – 30 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.

(6 marks)

b) Most developers are aware that they should never store plaintext passwords in a database and usually resort to storing MD5 or SHA1 hashes of the password.

i. Explain why developers should never just use an unsalted hash of a password in their databases. **(3 marks)**

ii. Explain why using salted MD5 or SHA1 hashes should also be avoided and what is the best method developers should deploy in their coding. **(4 marks)**

c) Most forensic investigators usually verify the integrity of their digital assets using either an MD5 or SHA1 hash.

i. Describe why using a single hash for the verification of forensic data is an unwise approach and describe how it may lead to a legal challenge against the evidence. **(4 marks)**

ii. How should the integrity of the forensic data be verified? **(2 marks)**

d)

i. Explain why collisions, although undesirable, are a mathematic certainty for practically all modern cryptographic hashing algorithms. **(3 marks)**

ii. In what scenario is it possible to avoid collisions completely. **(2 marks)**

iii. What is the name given to these collision free hashing algorithms. **(1 mark)**

e) Describe the strict avalanche criterion and explain why it is a desirable property for a cryptographic hash function.

(5 marks)

Question 3 (Digital Signatures– 30 Marks)

a) A company has decided to implemented email signatures for all employees. The company has created its own self signed root certificate, which it uses for signing all employee certificates.

i. While email signatures appear to be working internally external clients are complaining of certificate errors. What is the likely cause of this problem and how should the company address the issue. **(3 marks)**

ii. Could the company use its existing setup to encrypt (as well as sign) all internal emails? Explain your answer. **(3 marks)**

iii. What security mechanisms do digital signature offer. **(3 marks)**

iv. How might an attacker bypass email signatures to send faked emails? **(3 marks)**

b) Describe the process of signing a document to create a digital signature and detail how the recipient would verify the signed document.

(10 marks)

c) 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)

Question 4 (Secure Socket Layer – 30 Marks)

a) 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)

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

(6 marks)

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

(6 marks)

d) In recent years there have been a number of high profile attacks against various SSL/TLS implementations. List and describe in detail any three of these attacks.

(10 marks)