Institute of Technology Blanchardstown
Institiúid Teicneolaíochta Baile Bhlainséir

INSTITUTE OF TECHNOLOGY BLANCHARDSTOWN

Year	Year 1
Semester	Semester 1
Date of Examination	Tuesday 22nd Jan 2013
Time of Examination	3.30pm – 5.30pm

Prog Code	BN518	**Prog Title**	Master of Science in Computing	**Module Code**	MSIT H6020

Module Title	Secure Communications and Cryptography

Internal Examiners: *Mr Mark Cummins, Mr Mark Lane*
External Examiners: *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) **Question one in Section A is compulsory. Candidates should attempt all parts of question one and ANY other two questions from Section B.**
3) **This paper is worth 100 marks. Question 1 is worth 40 marks and all other questions are worth 30 marks each.**
4) **Answers to each question must start on a new page.**

DO NOT TURN OVER THIS PAGE UNTIL YOU ARE TOLD TO DO SO

Section A: Compulsory Question *(40 marks in total)*

Question 1: Attempt all parts of this question *(5 marks each)*

(a) Describe the *CIA Security model* and discuss an extra element which could be added to improve the model.

(5 marks)

(b) 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 affected, if a solution to either of these problems was discovered tomorrow?

(5 marks)

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

(5 marks)

(d) 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)

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

(5 marks)

(f) 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)

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

(5 marks)

(h) Briefly compare and contrast symmetric and asymmetric encryption.

(5 marks)

Section B: Answer ANY two questions

Question 2: *(30 Marks)*

(a) Describe, using an example, how Alice and Bob, who have no previous knowledge of each other, can use the Diffie-Hellman key exchange (D-H) to jointly establish a shared secret key over an insecure communications channel.

(12 marks)

(b) Explain how the Diffie-Hellman key exchange is vulnerable to man-in-the-middle attacks. What additional mechanism is usually implemented with Diffie-Hellman to help protect against man-in-the-middle attacks?

(8 marks)

(c) List and briefly describe the six threats to communications security (or STRIDE model). Describe how cryptographic countermeasures can be combined to secure against these threats.

(10 marks)

Question 3: (30 marks)

(a) Describe the common threats to secure browsing on the Internet, and with the aid of a diagram show how TOR and Hypertext Transfer Protocol Secure (HTTPS) can be combined to provide more anonymous browsing capabilities.

(12 marks)

(b) Two security options commonly used by WLAN administrators include mac address filtering and disabling SSID broadcasts. Show the weakness in each of these security mechanisms by describing in detail how an attacker could easily bypass each of these two mechanisms.

(9 marks)

(c) The X.509 standard covers a broad range of components of the public key infrastructure. Most notably, it describes a standard format for digital certificates. List and describe the required components of an X.509 certificate.

(9 marks)

Question 4: (30 marks)

(a) Describe how the Transport Layer Security/Secure Sockets Layer protocol (TLS/SSL) can be used to secure a HTTP communication session between a client and server.

(12 marks)

(b) Describe how the simple Caesar Cipher is incorporated into the Vigenère cipher to form a more complex form of encryption, and demonstrate the use of the Vigenère cipher to encrypt the plaintext *TECHNOLOGY* using the key *DOG*
Note: a copy of the Vigenère square is provided over the page.

(8 marks)

(c) Alice and Bob wish to communicate securely with each other. Describe how they can use digital signatures to ensure authentication, message integrity and non-repudiation between themselves.

(10 marks)

Appendix A:

Vigenère square (for use in Section B, Question 4 (b)).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y