DUBLIN CITY UNIVERSITY

SEMESTER TWO EXAMINATIONS 2008

MODULE: ***(Title & Code)***	Internetwork Security (EE548)
COURSE:	M.Eng. in Electronic Systems (MEN) Grad. Dip. in Electronic Systems (GDE) M.Eng. in Telecommunications Eng. (MTC) Grad. Dip. in Telecommunications Eng. (GTC) Grad. Cert. in Telecommunications Eng. (GCTC) Study Abroad (Engineering and Computing) (ECSAX)
YEAR:	C
EXAMINERS:	Mr. Damien O'Rourke Prof. Paul Rees
TIME ALLOWED:	3 Hours
INSTRUCTIONS:	Please answer any **FOUR** questions[1]. All questions carry equal marks

Requirements for this paper
Please tick (X) as appropriate

- ___ ***Log Table***
- ___ ***Graph Paper***
- ___ ***Attached Answer Sheet***
- ___ ***Statistical Tables***
- ___ ***Floppy Disk***
- ___ ***Actuarial Tables***

THE USE OF PROGRAMMABLE OR TEXT STORING CALCULATORS IS EXPRESSLY FORBIDDEN

PLEASE DO NOT TURN OVER THIS PAGE UNTIL YOU ARE INSTRUCTED TO DO SO

[1] *Please note that where a candidate answers more than the required number of questions, the examiner will mark all questions attempted and then select the highest scoring ones.*

Question 1

(a) Define what is meant by the following:

(i) A Security service
(ii) A Security mechanism
(iii) Nonrepudiation
(iv) Authentication [4 marks]

(b) (i) Use the Playfair matrix shown in figure 1 to encrypt the following plaintext:

Must see you over Cadogan West. Coming at once.

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

Figure 1: Playfair matrix for use in part (i) [6 marks]

(ii) Construct a **new** Playfair matrix with the key *largest*. [4 marks]

(iii) Encrypt the plaintext from part (i) with the Playfair matrix you obtained in part (ii). How do you account for the results of this problem? Can you generalise your conclusion? [5 marks]

(c) Draw a diagram of a three-cylinder Rotor machine and **briefly** explain how it works. [6 marks]

[Total marks: 25]

Question 2

(a) (i) Draw a detailed diagram of a **single DES round** (including the operations on the key). [7 marks]

(ii) Draw a detailed diagram of the AES cipher used for **decryption only**. [7 marks]

(iii) Briefly describe the mix columns operation used in the AES standard. [5 marks]

(b) Draw a detailed diagram of the ***Output Feedback Mode*** (OFB). What feature of this (and other) modes influenced the design of the AES algorithm? [6 marks]

[Total marks: 25]

Question 3

(a) Draw a detailed diagram of a key distribution scenario for a symmetric key cryptosystem with an initiator A, responder B and a Key distribution centre (KDC). State clearly the purpose of each step. [12 marks]

(b) Draw a diagram of the ANSI X9.17 Pseudorandom Number Generator and describe it's parameters. [7 marks]

(c) (i) Give three properties all random number **generators** should have. [3 marks]

(ii) How can a Pseudorandom Number Generator be used to Mitigate a traffic analysis? Use a diagram to help explain your answer. [3 marks]

[Total marks: 25]

Question 4

(a) (i) Briefly define what is meant by an abelian group.

(ii) Briefly define what is meant by a commutative ring.

(iii) What is meant by co-prime? Give another name for this expression.

(iv) Explain what is meant by a least residue.

(v) What is a residue class? [12 marks]

(b) Determine the result of the following operation:
$\{87\} \oplus (\{02\} \bullet \{6E\}) \oplus (\{03\} \bullet \{46\}) \oplus \{A6\}$

Where "$\bullet$" defines multiplication over GF(2^8) and the irreducible polynomial used is: $m(x) = x^8 + x^4 + x^3 + x + 1$

Why does the value of $m(x)$ given here have special significance in cryptography? [5 marks]

(c) Given two primes numbers p and q with $p \neq q$, show that $\phi(n) = (p-1) \times (q-1)$ where $n = p \times q$ and $\phi(n)$ is Euler's totient function. [8 marks]

[Total marks: 25]

Question 5

(a) (i) List **six** properties a hash function must have to be useful for message authentication. [6 marks]

(ii) List the steps of an attack on hash codes based on the birthday paradox. [5 marks]

(b) (i) Draw a detailed diagram of the **general** structure of a Secure Hash code. [7 marks]

(ii) Draw a detailed diagram of message digest generation using SHA-512. [7 marks]

[Total marks: 25]

Question 6

(a) Give a detailed description of a differential power analysis attack. [13 marks]

(b) Give **four** techniques that can be used to mitigate a power analysis attack with a brief description of each. [8 marks]

(c) Give a brief definition for each of the following terms:

1. Unconditionally Secure
2. Computationally Secure
3. Cryptanalytic Attack
4. Implementation Attack [4 marks]

[Total marks: 25]