# *DUBLIN CITY UNIVERSITY*

## *SEMESTER TWO EXAMINATIONS 2007*

| | |
|---|---|
| ***MODULE:*** ***(Title & Code)*** | Internetwork Security (EE548) |
| ***COURSE:*** | M.Eng. in Electronic Systems (MEN)<br>Grad. Dip. in Electronic Systems (GDE)<br>M.Eng. in Telecommunications Eng. (MTC)<br>Grad. Dip. in Telecommunications Eng. (GTC)<br>Grad. Cert. in Telecommunications Eng. (GCTC)<br>Individual Postgrad. Modules-Electronics (IPMEC) |
| ***YEAR:*** | 1 |
| ***EXAMINERS:*** | Mr. Damien O'Rourke (Ext: 8514)<br>Prof. Paul Rees |
| ***TIME ALLOWED:*** | 3 Hours |
| ***INSTRUCTIONS:*** | Please answer any **FOUR** questions[1].<br>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) Use the Vigenère square of Figure 1 (last page of this booklet) to determine the plaintext given the following information:

**Ciphertext:** *arncbdgigjzqxlxugtmgkipvrlhpie*
**Key word:** *encrypt* [5 marks]

(b) Use the **Playfair cipher** to encrypt the following plaintext with the key word provided:

**Plaintext:** I will travel by sea in the morning
**Key word:** *security* [8 marks]

(c) Describe in detail **five** block cipher modes of operation. [12 marks]

[Total marks: 25]

## Question 2

(a) For cryptographic applications it makes some sense to make use of the encryption logic available to produce random numbers. The pseudo-random number generator specified in ANSI X9-17 is employed in many such applications. Give a brief overview of this scheme along with a block diagram of the generator. [10 marks]

(b) Describe the **Linear Congruential Method (LCM)** for the generation of pseudo-random number sequences. What are the limitations of LCM when applying the technique in cryptographic applications? How might this method be improved? [10 marks]

(c) Give three proposed criteria a good pseudorandom number generator should adhere to. [5 marks]

[Total marks: 25]

**Question 3**

(a) Explain in detail what is meant by the "Big O" notation and discuss how it is used in computer science. [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? [7 marks]

(c) Show that $\gcd(a,b) = \gcd(b, a \bmod b)$ for any integers $a$ and $b$. [6 marks]

[Total marks: 25]

**Question 4**

(a) Describe the **RSA algorithm** and illustrate how the public and private keys are generated. [12 marks]

(b) Making use of the extended version of Euclid's algorithm, perform encryption of the plaintext message M using the RSA algorithm with the following parameter values:-

Primes p = 2, q = 11;
Plaintext M = 2;
Value of the public key e = 7.

to produce ciphertext C. Using C perform the decryption to verify your answer. [5 marks]

(c) Describe the main ingredients of the Knapsack scheme developed by Ralph Merkle saying whether each value is private, public, chosen or calculated. [8 marks]

[Total marks: 25]

## Question 5

(a) Outline the architecture and main elements of the **Secure Sockets Layer (SSL)** protocol. [12 marks]

(b) When a Web Server authenticates itself to a browser in an SSL handshake, it uses **X.509 certificates** to do so. Outline the format of an X.509 certificate and very briefly explain each field. [8 marks]

(c) The X.509 version 2 format does not convey all of the information that recent design and implementation experience has shown to be needed. Give **five** requirements that are not satisfied by version 2 along with a very brief explanation of each. [5 marks]

[Total marks: 25]

## Question 6

(a) Give a detailed description of how a differential power analysis attack works. [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]

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

Figure 1: Vigenère Square used in **Q1a**.