MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2014/2015

TSN3251 and TSC2211 – COMPUTER SECURITY

(All Sections / Groups)

26 SEPTEMBER 2014
3:00 p.m. – 5:00 p.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 6 pages (including cover page) with 7 Questions only.

2. Attempt **SIX** out of **SEVEN** questions. The distribution of the marks for each question is given. This paper carries **60 marks**.

3. Please print all your answers in the Answer Booklet provided.

Question 1 (10 Marks)

a) In the effectiveness of security controls, state the "Principle of Effectiveness".

[1 mark]

b) Threats can be broadly classified into FOUR (4) types. TWO (2) of them are interception and interruption. What are the other two and give a brief explanation for all FOUR (4) types.

[4 marks]

c) Cryptographic ciphers can be categorized into symmetric and asymmetric types. Briefly explain the difference between the two categories.

[2 marks]

d) Give three specific applications that can be addressed by asymmetric cryptography.

[3 marks]

Question 2 (10 Marks)

a) Encrypt the following sentence using Caesar cipher where $C_i = P_i + 5$.

"who won the world cup this year"

In your answer, copy the following table to show how you did your encryption.

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

[3 marks]

b) Explain the use of Frequency Distribution (also known as Index of Coincidence) in decrypting a ciphertext that has been encrypted using substitution cipher.

[2 marks]

Continued ...

a) The ciphertext RTGI was encrypted by a Hill cipher with the key $\begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix}$. Find the plaintext. Show your steps clearly.

[5 marks]

Question 3 (10 Marks)

a) Briefly explain the difference between substitution and transposition encryption.

[1 mark]

b) The Playfair cipher is based on the use of a 5 x 5 matrix constructed using a keyword. The plaintext is then encrypted in pairs (two at a time) using this matrix. Explain the rules of encryption.

[2 marks]

c) Using the Playfair cipher, encrypt the following text using the key "seamus". Show the 5 x 5 matrix constructed and the pairing of the letters for encryption.

I saw nothing at the zoo today

[3 marks]

d) Given the following ciphertext, decrypt it using a 3 row rail fence transposition cipher.

KADFIOENAISAHORLESN

[4 marks]

Question 4 (10 Marks)

a) What is meant by the Avalanche Effect in an encryption algorithm?

[1 mark]

b) Use the Extended Euclidean Algorithm to compute the multiplicative inverse of 101 mod 17. Show each step clearly.

[3 marks]

Continued ...

c) Miller Rabin Algorithm is a test based on the Fermat's Theorem. The Miller-Rabin Algorithm is as described below.

TEST (n) is:

1. Find integers k, q such that $k > 0$, q is an odd number, so that $(n-1)=2^k q$
2. Select a random integer a, where $1 < a < n-1$
3. if $a^q \bmod n = 1$ then return ("maybe prime");
4. for $j = 0$ to $k - 1$ do
   5. if $(a^{2^j q} \bmod n = n-1)$
      then return("maybe prime")
6. return ("composite")

Using the algorithm above, show how you will test for the number 13 by choosing the random integer a 3 times.

[5 marks]

d) Why are probabilistic considerations required when using the Miller-Rabin Algorithm?

[1 mark]

Question 5 (10 Marks)

a) Programmers do make errors that can cause program malfunctions and a few classes of errors have plagued programmers and security professionals for decades. Three (3) classic error types that have enabled many security breaches are (i) Buffer Overflows, (ii) Incomplete Mediation, and (iii) Time-of-Check to Time-of-Use Errors. Explain any two (2) of the error types listed

[2 marks]

b) Briefly describe the following three software threats.

- Virus
- Worms
- Trap Doors

[3 marks]

Continued ...

c) Describe THREE (3) basic security requirements of a database?

[3 marks]

d) There are TWO (2) main methods to protect against inference attacks. List the TWO methods and provide an explanation for each one.

[2 marks]

Question 6 (10 Marks)

a) Provide at least FOUR (4) guiding statements for selecting and maintaining good passwords.

[2 marks]

b) In Operating System Access Security, what is the principle of least privilege? Why is it important?

[3 marks]

c) In network security threats, explain the following terms.

   a. Phishing in Man-in-the-Middle attacks
   b. Ping of Death in Denial of Service (DoS) attacks
   c. SYN Flooding in Denial of Service (DoS) attacks

[3 marks]

d) Intrusion Detection Systems (IDS) can be broadly categorized into FOUR (4) types: Signature Based, Anomaly Based, Network Based and Host Based. Describe Anomaly Based IDS and give at least (1) ONE advantage of using Anomaly Based IDS as opposed to Signature Based IDS.

[2 marks]

Continued ...

Question 7 (10 Marks)

a) Give SIX (6) issues which should be addressed by a security plan.

[6 marks]

b) Define Intellectual Property.

[1 mark]

c) Explain Copyrights, Patents and Trade Secrets.

[3 marks]

END OF EXAM PAPER