MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2015/2016

TSN3251 – COMPUTER SECURITY

(All Sections / Groups)

16 OCTOBER 2015
3:00 p.m. – 5:00 p.m.
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This paper consists of 7 pages (including cover page) with 5 Questions only.

2. Attempt **ALL FIVE** questions. The distribution of the marks for each question is given. This paper carries **100 marks**.

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

Question 1 (20 Marks)

a) In computer security, in addition to securing the system software, name FOUR (4) other broad areas that require securing.

[4 marks]

b) Confidentiality, integrity and availability (CIA), is a model designed to guide policies for information security within an organization. In your own words, explain and give an example each on what is meant by the THREE (3) terms: **confidentiality**, **integrity** and **availability**.

[6 marks]

c) Briefly explain the terms used to classify threats: Interception, Interruption, Modification and Fabrication.

[4 marks]

d) A "threat" is an attacker (can be a person or a machine) and "vulnerabilities" are the weak points in the system. Using those two terms, "threat" and "vulnerabilities", briefly define what "controls" are in the system.

[2 marks]

e) What are the FOUR (4) categories (types) of computer criminals?

[4 marks]

Continued ...

Question 2 (20 Marks)

a) Encrypt the following sentence with key substitution cipher using the key "WAGAMAMA".

"i am going to ace this exams"

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

[4 marks]

b) Given the encrypted text (C) "SRSD" that was encrypted using the Hill Cipher with the key (K) "VPAF" (using $C = P \cdot K$), deduce the plaintext (P). (Hint: You will need K^{-1})

[9 marks]

c) Decipher the following text that was encrypted using a 3 row rail fence cipher.

ITRFWNTBEKREAOAE

[3 marks]

d) Decrypt the following that has been encrypted using a three columnar transposition method.

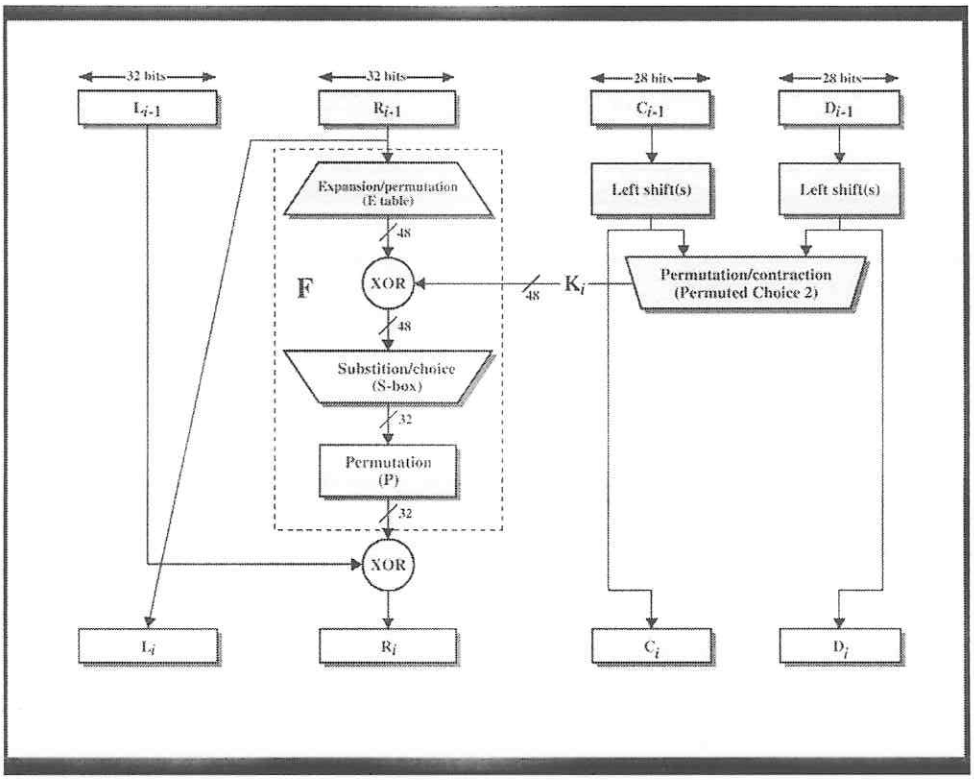
IDTOLDMURSIYTI

[4 marks]

Continued ...

Question 3 (20 Marks)

a) Consider the Single Round of Data Encryption Standard (DES) Algorithm as depicted in the figure below.



Given C_8 is "1101 1101 1101 0011 0101 0111 1111", compute the value of C_9. The schedule of left shifts and the table for Permuted Choice 2 (PC-2) is as below.

[2 marks]

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Schedule of Left Shifts

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Permuted Choice 2 (PC-2)

Continued ...

b) Referring to the Single Round of Data Encryption Standard (DES) Algorithm: Given that L_3 is "1111 1111 0000 0001 0011 0110 0010 1111" and R_3 is "1101 1101 1101 0011 0101 1101 1010 1101". Use the *E Table* to compute the output after the Expansion/Permutation stage.

[5 marks]

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Expansion/Permutation (E)

c) State the Extended Euclidean Algorithm (in Pseudo Code). Use the Extended Euclidean Algorithm to compute the multiplicative inverse of 3 mod 11. Show each step clearly.

[7 marks]

d) RSA is the best known and most widely used algorithm for Public Key Cryptography. Describe the steps for RSA Key Generation.

[6 marks]

Continued ...

Question 4 (20 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 all three (3) of the listed error types.

[6 marks]

b) Describe the following FIVE (5) software threats.

- Virus
- Worms
- Trap Doors
- Logic Bomb
- Rabbit

[5 marks]

c) Give an overview of Database SQL Injection attack. (You may use code snippet to explain if needed).

[5 marks]

d) In contingency planning, explain what are (i) cold backup sites and (ii) hot backup sites.

[4 marks]

Question 5 (20 Marks)

a) For Operating System's memory protection, explain what is meant by the following terms:-

i. Fence

ii. Relocation

Use diagrams to illustrate it if needed.

[4 marks]

Continued ...

b) Give a brief explanation of any TWO (2) drawbacks of using passwords as a form of authentication.

[2 marks]

c) Differentiate between a Host Based Intrusion Detection System (IDS) and a Network Based IDS. Explain why a Host Based Intrusion Detection System (IDS) is more expensive to implement in a large organization as compared to Network Based IDS.

[2 marks]

d) There are many types of Denial of Service (DOS) attacks; other than "Ping of Death" and "Spam", state TWO (2) other techniques and provide detailed explanations on how they work. (For each of the type of DOS; 1 mark for the naming of the DOS attack technique and 2 marks for the detailed explanation).

[6 marks]

e) Provide the proper means of legal protection that can be applied for the following scenarios. Justify your answer on how the protection will be beneficial.

i) Maria developed a new iOS application and she would like to publish it but would like to protect his Intellectual Property prior to doing so.

ii) A scientist, Professor Chuah, has drafted out a new method to filtrate river water for drinking purposes. He would like to produce and commercialise it under the name CleanH_20. What are the means of legal protections necessary in this case?

iii) Selva has successfully commercialized his point of sale software and it is relatively well known in the market as BizzyBee. How can he ensure that no other person or company will use the same product name?

[6 marks]

END OF EXAM PAPER