Infrastructure University Kuala Lumpur

FINAL EXAMINATION
JUNE SEMESTER 2019

NETWORK AND DATA SECURITY
(CSC 2730)

(TIME: 3 HOURS)

MATRIC NO. : | | | | | | | | | |

IC. / PASSPORT NO. : | | | | | | | | | | | | | | |

LECTURER : **CHIRANJIBI ADHIKARI**

GENERAL INSTRUCTIONS

1. This question booklet consists of **5 printed** pages including this page.
2. Answer **ALL questions** in **Section A** in the **ANSWER BOOKLET**.
3. Answer **ANY TWO (2)** questions in **Section B** in the Answer Booklet.
4. **PLEASE DO NOT TURN THIS PAGE AND START THE EXAM UNTIL YOU ARE TOLD TO DO SO.**

INSTRUCTIONS: **TIME: 3 *HOURS***

SECTION A **(60 MARKS)**

There are SEVEN (7) questions in this section. Answer ALL Questions in the Answer Booklet.

1. Discuss **THREE (3)** objectives of computer security.

(6 marks)
(CLO1:PLO1:C1)

2. Define the following terms:
   a) Firewall

(2 marks)

   b) Dictionary Attack

(2 marks)

   c) Intrusion Detection

(2 marks)

   d) Denial of Service

(2 marks)
(CLO1:PLO1:C1)

3. Discuss the term passive attack and active attack.

(4 marks)
(CLO2:PLO2:C3)

4. Ceaser Cipher is the simplest substitution cipher, introduced by Julius Ceaser.
   a) Briefly explain on the substitution technique in Ceaser Cipher.

(2.5 marks)
(CLO3:PLO4:C2)

   b) Encrypt the following plaintext with the given key using Ceaser Cipher.
   Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
   Key: 15

(17.5 marks)
(CLO3:PLO4:C2)

5. List **THREE (3)** threats that exists in Kerberos.

(6 marks)
(CLO1:PLO1:C1)

6. Define the following terms in the context of security.
   a) Availability

   (2 marks)

   b) Adaptability

   (2 marks)

   c) Usability

   (2 marks)
   (CLO1:PLO1:C1)

7. Illustrate a fully labelled diagram /model of network security.

   (10 marks)
   (CLO3:PLO4:C2)

INSTRUCTIONS: **TIME: 3 *HOURS***

SECTION B **(40 MARKS)**

There are THREE (3) questions in this section. Answer ANY TWO (2) Questions in the Answer Booklet.

1.

a) Briefly describe any **TWO (2)** types of attacks that can be categorized as an Active Attack.

(4 marks)
(CLO2:PLO3:C3)

b) Discuss **THREE (3)** key concepts in Kerberos version 4.

(6 marks)
(CLO2:PLO3:C3)

c) Employees are increasingly connecting to company networks remotely via mobile devices such as laptops, tablets and smartphones. Remote access needs to satisfy five essential requirements to be efficient and secure. Identify and briefly explain each of these **FIVE (5)** requirements.

(10 marks)
(CLO2:PLO3:C3)

2.

a) Briefly explain Advanced Encryption System (AES) and the steps/rounds involved in the encryption.

(4 marks)
(CLO2:PLO3:C3)

b) With the given matrics (refer to Figure 1), perform the first TWO (2) rounds in an AES encryption to retrieve the cipher text. Show the working for each step. Refer to the S-Box given Table 1.

ad	f0	5d	df
b3	b9	c6	b2
6a	09	52	7a
Aa	7f	e2	3c

Figure 1

(16 marks)
(CLO2:PLO3:C3)

Table 1: AES standard S-Box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	28	76	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

3.

a) Define Diffie-Hellman Algorithm.

(5 marks)
(CLO2:PLO3:C3)

b) Alex and Bryan are transmitting data using Diffie-Hellman Algorithm. They have agreed to use a prime number p=47 and base g=11. Alex has chosen his secret integer, a=9 and Bryan has chosen his secret integer, b=15. Determine the secret key between Alex and Bryan.

(12 marks)
(CLO2:PLO3:C3)

c) State any **THREE (3)** difference between Symmetric and Asymmetric key encryption.

(3 marks)
(CLO2:PLO3:C3)

***** END OF QUESTIONS *****