E-ASSESSMENT_BAIT1093_(MAIN) 202003_KL

Questions Responses 21 Total points: 100

Section 1 of 6

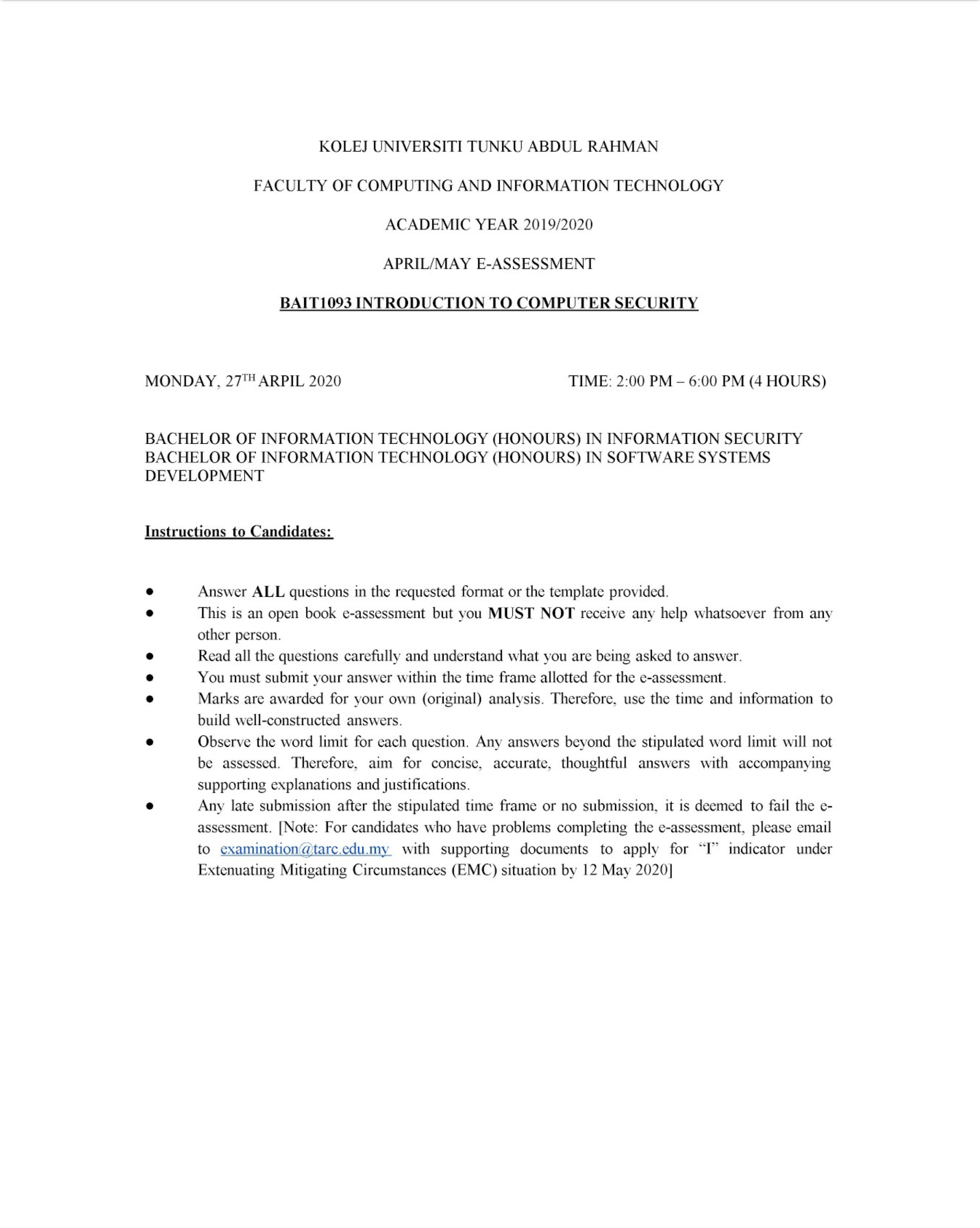
E-ASSESSMENT: BAIT1093

Form description

This form is automatically collecting email addresses for Tunku Abdul Rahman University College users. Change settings

Instruction to Candidate

Instruction to Candidate



KOLEJ UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY

ACADEMIC YEAR 2019/2020

APRIL/MAY E-ASSESSMENT

BAIT1093 INTRODUCTION TO COMPUTER SECURITY

MONDAY, 27TH ARPIL 2020 TIME: 2:00 PM – 6:00 PM (4 HOURS)

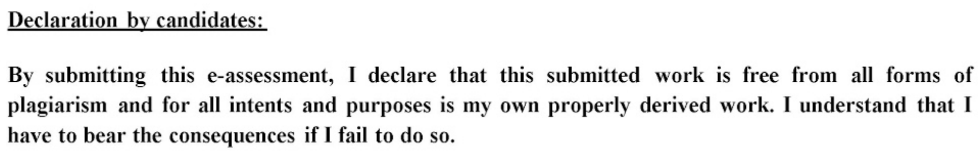
BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN INFORMATION SECURITY
BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN SOFTWARE SYSTEMS DEVELOPMENT

Instructions to Candidates:

- Answer **ALL** questions in the requested format or the template provided.
- This is an open book e-assessment but you **MUST NOT** receive any help whatsoever from any other person.
- Read all the questions carefully and understand what you are being asked to answer.
- You must submit your answer within the time frame allotted for the e-assessment.
- Marks are awarded for your own (original) analysis. Therefore, use the time and information to build well-constructed answers.
- Observe the word limit for each question. Any answers beyond the stipulated word limit will not be assessed. Therefore, aim for concise, accurate, thoughtful answers with accompanying supporting explanations and justifications.
- Any late submission after the stipulated time frame or no submission, it is deemed to fail the e-assessment. [Note: For candidates who have problems completing the e-assessment, please email to examination@tarc.edu.my with supporting documents to apply for "I" indicator under Extenuating Mitigating Circumstances (EMC) situation by 12 May 2020]

Declaration by candidates

Declaration by candidates



Declaration by candidates:

By submitting this e-assessment, I declare that this submitted work is free from all forms of plagiarism and for all intents and purposes is my own properly derived work. I understand that I have to bear the consequences if I fail to do so.

After section 1 Continue to next section

Section 2 of 6

Student Information

You are required to provide accurate information.

Student ID (Example: 19WADXXXXX) *

Short answer text

Student Name (in capital letters) *

Short answer text

Programme *

○ RIS

○ RSD

○ REI

Semester *

○ 1

○ 2

○ 3

Year *

○ 1

○ 2

After section 2 Continue to next section

Section 3 of 6

Question 1

Answer ALL Questions. Total 25 marks.

a) Explain TWO (2) accessory security concepts which required to elucidate the succeed in the computer security requisites. (4

Long answer text

b) (i) Attack can be categorized as passive attack and active attack. Discuss those attacks that are carried out and leads to an undesirable violation of security, or threat consequence.

Long answer text

b) (ii) With appropriate examples, illustrate ONE (1) category of passive attack and ONE (1) category of active attack on how those attacks are carried out. [Note: Your answers are to be in written form, take photo of your answers, put your answers in MS Word, convert to PDF file and then upload the PDF file. Maximum PDF file size is 1 MB. PDF file name format is "StudentName_QuestionNumber"] (6 marks)

Add file

c) (i) Briefly describe THREE(3) classification of disseminate malware which are arguably constitutes one of the most significant categories of threats to computer systems.

Long answer text

c) (ii) Classify the FOUR (4) primary components of prevention which are the ideal solution to the threat of malware. (4

Long answer text

c) (iii) With an example, clarify ONE(1) category of payloads which is aiming on integrity and availability. (4

Long answer text

After section 3 Continue to next section ▾

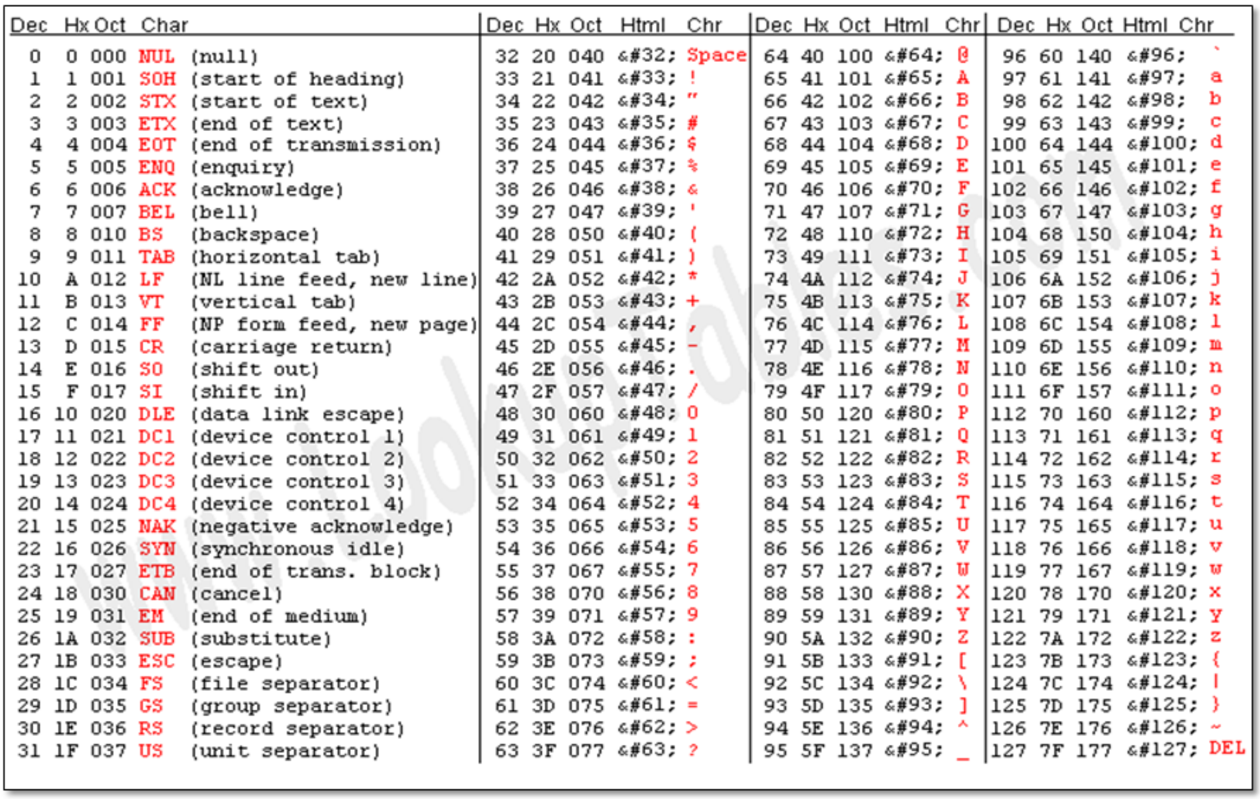
Section 4 of 6

Question 2

Answer ALL Questions. Total 25 marks.

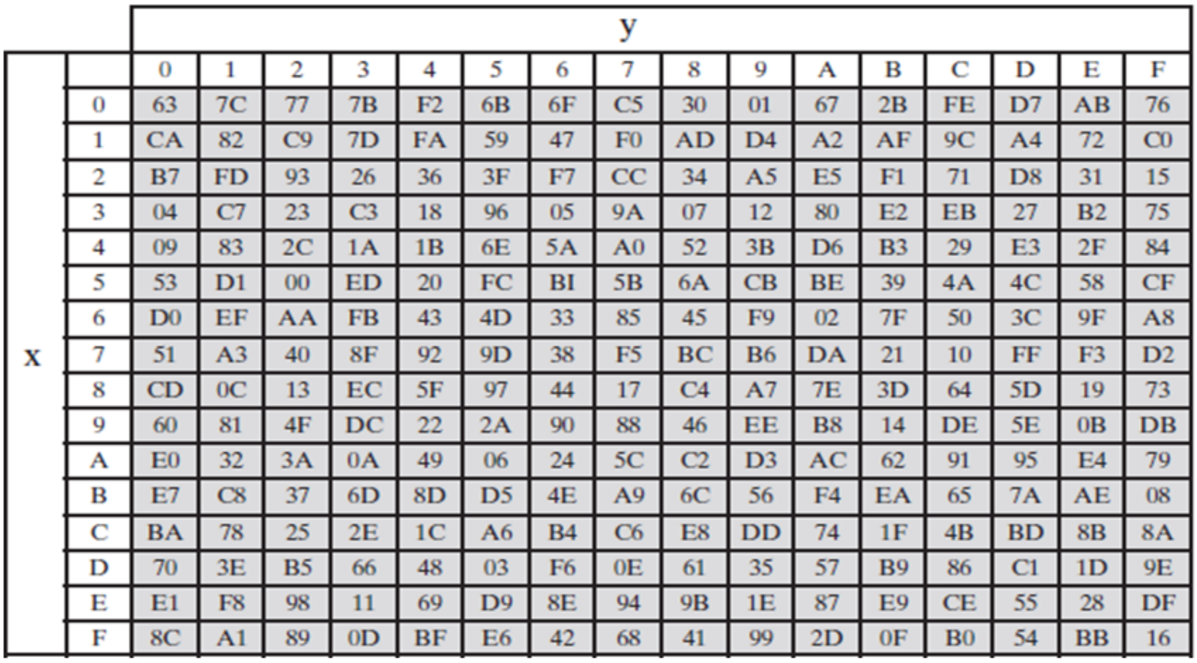
a) (i) Advanced Encryption Standard (AES) is a block cipher. The AES uses cryptographic keys to encrypt and decrypt data. AES does not use a Feistel structure but processes the entire data block in parallel using substitutions and permutation. Perform substitute byte transformation and shift row transformation for the following plaintext by displaying the byte values in matrix.
Plaintext: Hello Buddy Cool

[Note: refer to Table 1: ASCII Table and Table 2: AES S-Box. MUST show your workings of each transformation. Your answers are to be in written form, take photo of your answers, put your answers in MS Word, convert to PDF file and then upload the PDF file. Maximum PDF file size is 1 MB. PDF file name format is "StudentName_QuestionNumber"]
(6 marks)



Dec	Hx	Oct	Char		Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL	(null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH	(start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX	(start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX	(end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT	(end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ	(enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK	(acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL	(bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS	(backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB	(horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF	(NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT	(vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF	(NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR	(carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO	(shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI	(shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE	(data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1	(device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2	(device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3	(device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4	(device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK	(negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN	(synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB	(end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN	(cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM	(end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB	(substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC	(escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS	(file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS	(group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS	(record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US	(unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Table 1: ASCII table



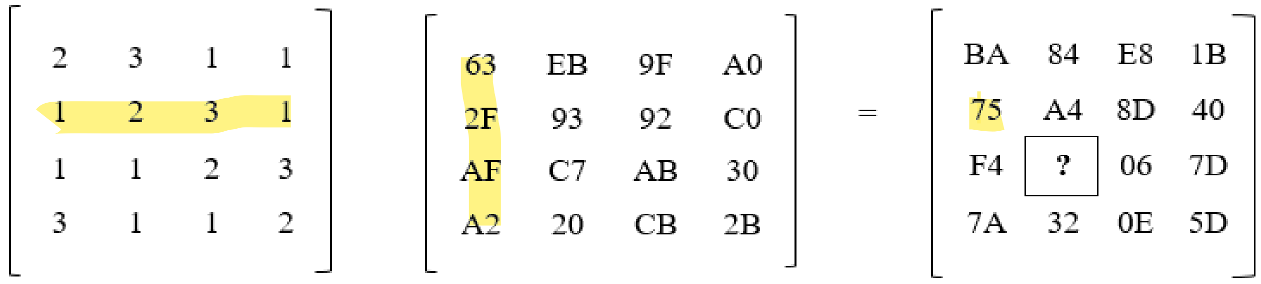
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	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

Table 2: AES S-Box

Add file

a) (ii) Given the following matrix of the current state, perform forward mix column

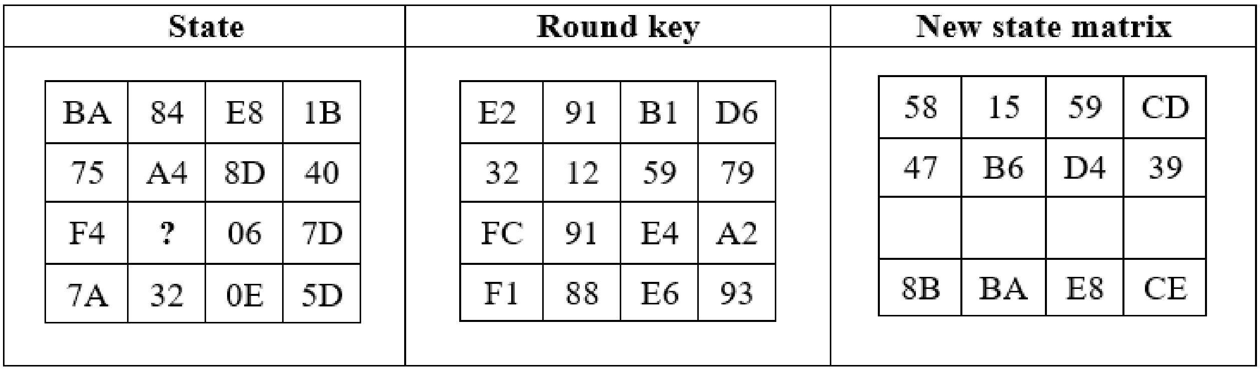
Maximum PDF file size is 1 MB. PDF file name format is "StudentName_QuestionNumber"]



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix} = \begin{bmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & \boxed{?} & 06 & 7D \\ 7A & 32 & 0E & 5D \end{bmatrix}$$

Add file

a) (iii) After successfully calculate and found the value of the empty field labeled “?” in the matrix in Question 2 a) (ii) is the first matrix called State. Now you will be given the second matrix which is Round key. You are required to perform forward add round key transformation to show the output of New state matrix of AES for the entire third row. [Note: MUST show the workings of calculation. Your answers are to be in written form, take photo of your answers, put your answers in MS Word, convert to PDF file and then upload the PDF file. Maximum PDF file size is 1 MB. PDF file name format is "StudentName_QuestionNumber"]



State				Round key				New state matrix			
BA	84	E8	1B	E2	91	B1	D6	58	15	59	CD
75	A4	8D	40	32	12	59	79	47	B6	D4	39
F4	?	06	7D	FC	91	E4	A2				
7A	32	0E	5D	F1	88	E6	93	8B	BA	E8	CE

Add file

b) (i) For information systems, the role of physical security is to protect the physical assets that support the storage and processing of information. Justify the classification of peril to the physical security triggered by technical threats.

Long answer text

b) (ii) Describe TWO (2) consideration for managing temperature and humidity which are infelicitous. (4

Long answer text

After section 4 Continue to next section ▼

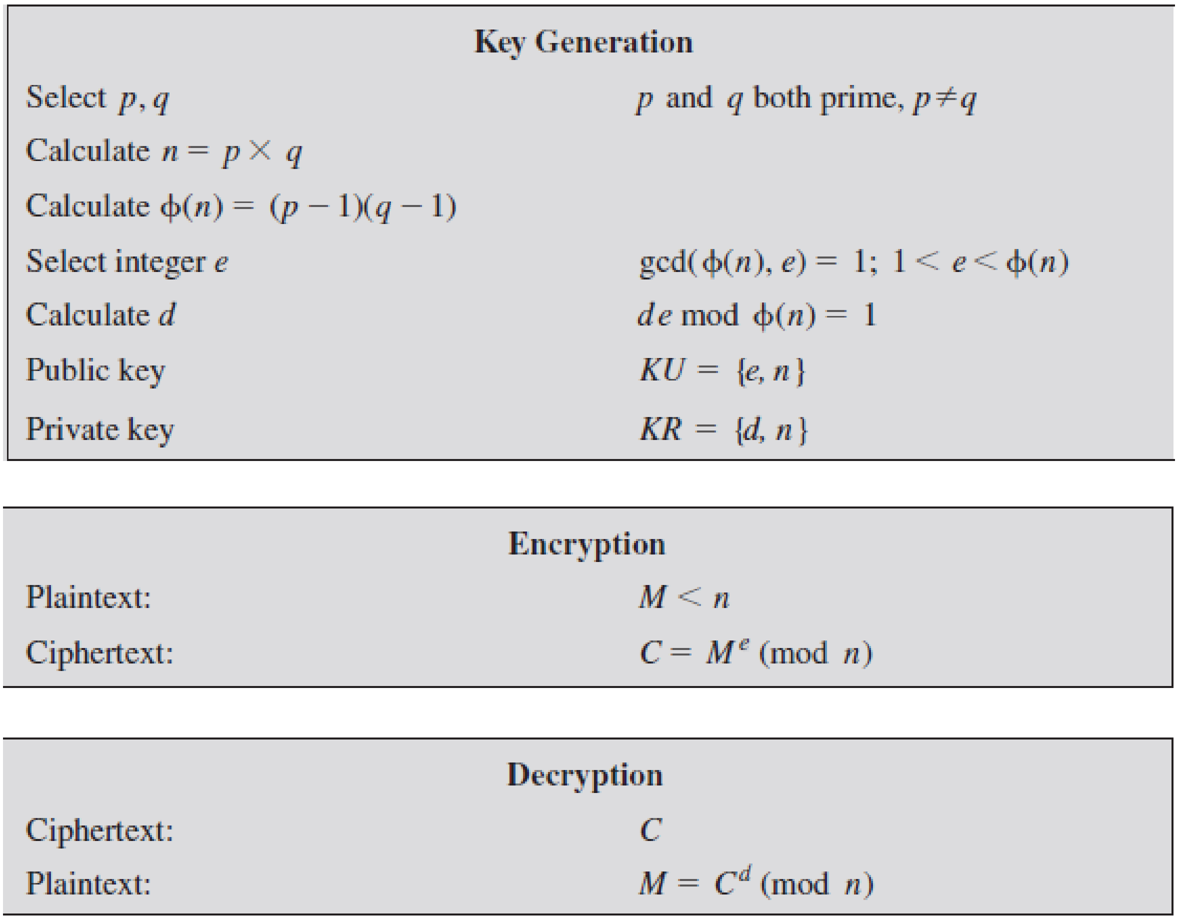
Section 5 of 6

Question 3

Answer ALL Questions. Total 25 marks.

a) (i) The RSA scheme has since that time reigned supreme as the most widely accepted and implemented approach to public-key encryption. Diffie-Hellman key exchange is to enable two users to exchange a secret key securely. Perform encryption and decryption using the RSA algorithm as in Figure 1, for the following:
p = 3; q = 17, e = 5; M = 5;

[Note: MUST show the workings of calculation to prove the answer is correct.]
(8 marks)



Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

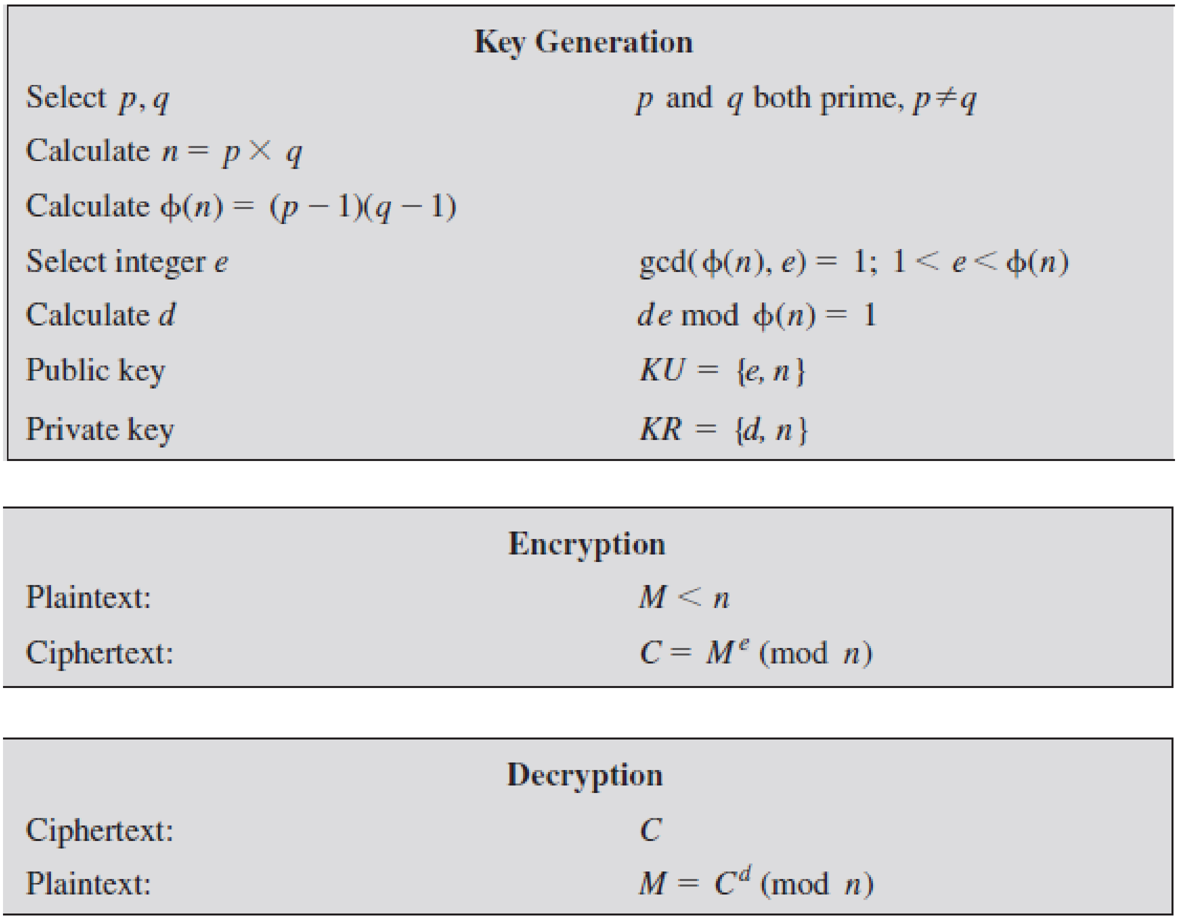
Figure 1: The RSA Algorithm

Long answer text

a) (ii) The RSA scheme has since that time reigned supreme as the most widely accepted and implemented approach to public-key encryption. Diffie-Hellman key exchange is to enable two users to exchange a secret key securely. Perform encryption and decryption using the RSA algorithm as in Figure 1, for the following:

p = 11; q = 13, e = 11; M = 7;

[Note: MUST show the workings of calculation to prove the answer is correct.]
(8 marks)



Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

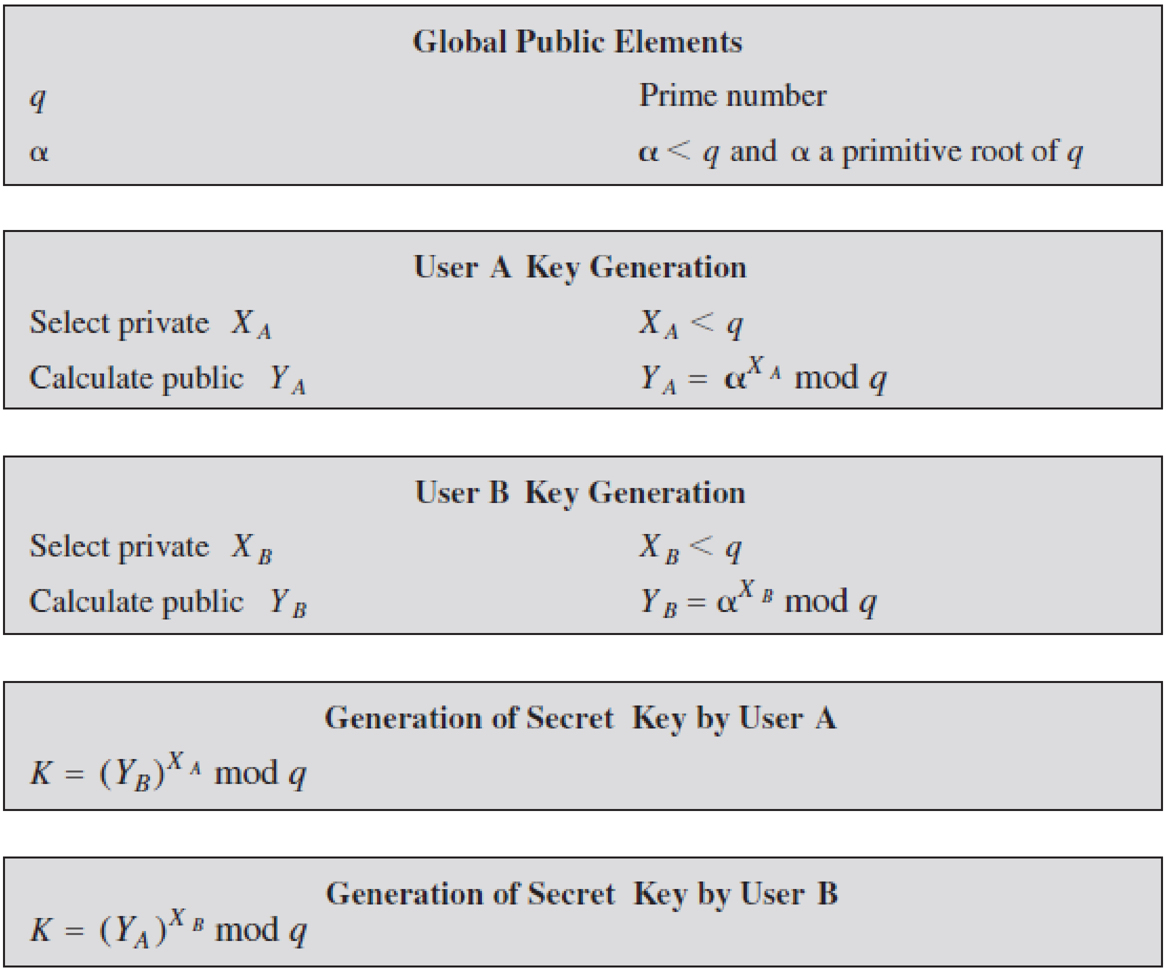
Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

Figure 1: The RSA Algorithm

Long answer text

b) (i) Consider a Diffie-Hellman scheme with a common prime q = 23 and a primitive root α = 5. Use the Diffie-Hellman Key Exchange Algorithm, as shown in Figure 2 for the following: Alice has public key YA = 10, what is Alice's private key XA?

[Note: MUST show the workings of calculation to prove the answer is correct.] (3 marks)



Global Public Elements

q	Prime number
α	$\alpha < q$ and α a primitive root of q

User A Key Generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$

Generation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$

Generation of Secret Key by User B

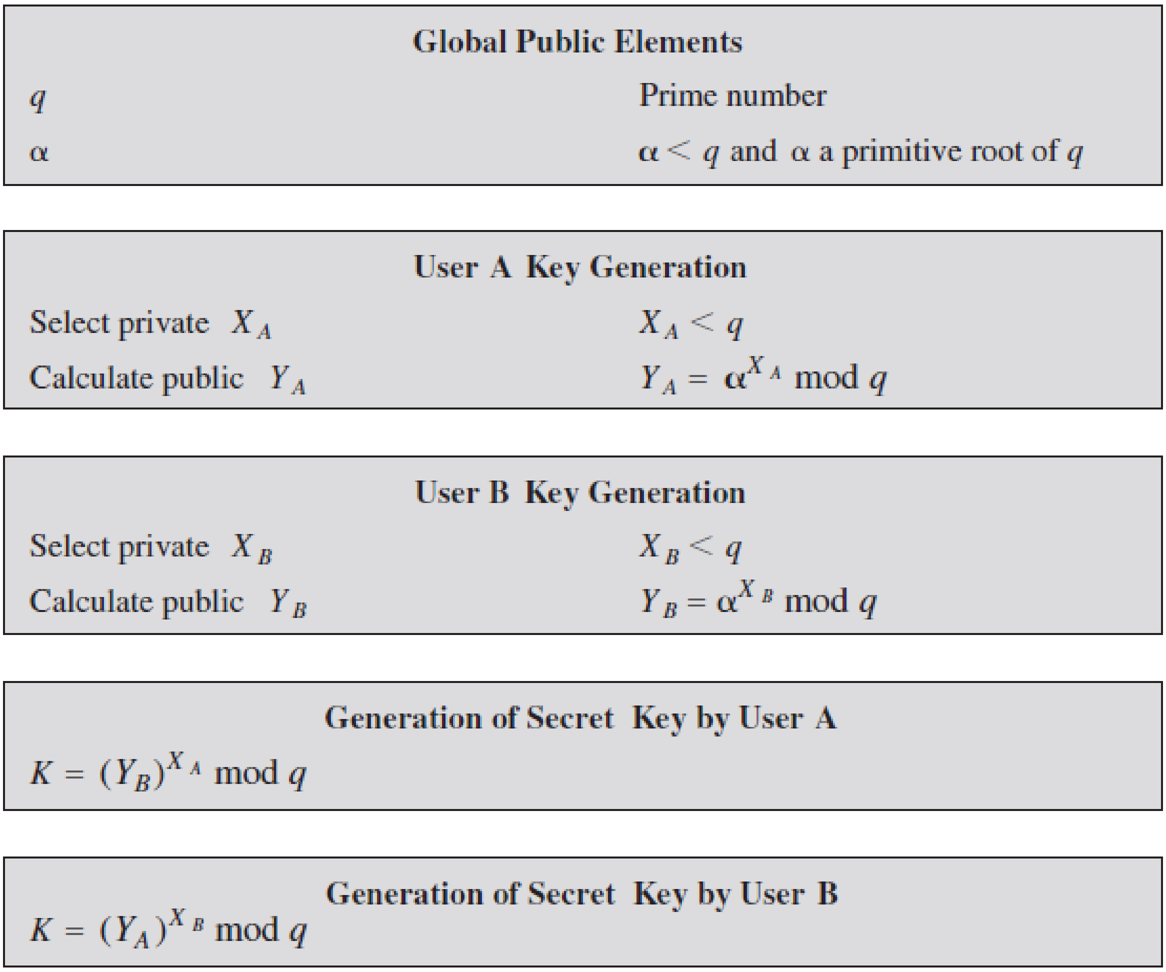
$K = (Y_A)^{X_B} \bmod q$

Figure 2: The Diffie-Hellman Key Exchange Algorithm

Long answer text

b) (ii) Use the Diffie-Hellman Key Exchange Algorithm, as shown in Figure 2 for the following: Bob has public key YB = 8, what is the shared secret key K?

[Note: MUST show the workings of calculation to prove the answer is correct.] (6 marks)



Global Public Elements

q Prime number

α $\alpha < q$ and α a primitive root of q

User A Key Generation

Select private X_A $X_A < q$

Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B $X_B < q$

Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$

Generation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$

Generation of Secret Key by User B

$K = (Y_A)^{X_B} \bmod q$

Figure 2: The Diffie-Hellman Key Exchange Algorithm

Long answer text

After section 5 Continue to next section

Section 6 of 6

Question 4

Answer ALL Questions. Total 25 marks.

a) Justify the suitability or unsuitability of the following passwords:

(i) Florida not suitable (2

a) Justify the suitability or unsuitability of the following passwords:

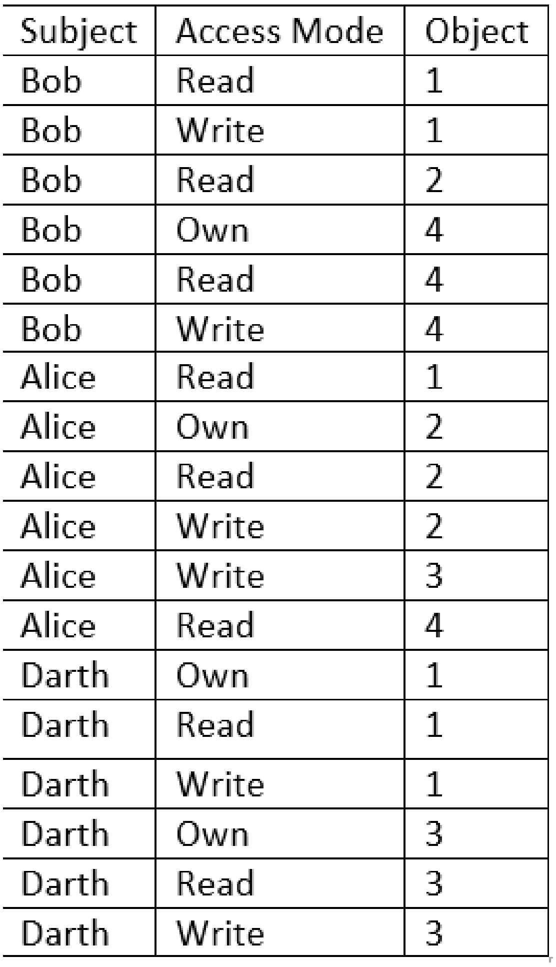
(ii) *laptop_admin# (2

Long answer text suitable

b) (i) Access control policy which can be embodied in an authorization database, dictates what types of access are permitted, under what circumstances and by whom. Access control policies are generally grouped into 4 categories. One of the category is Discretionary Access Control (DAC). Explain the requirements of DAC .

Long answer text

b) (ii) Table 3 is an Authorization Table for Files that contains one row for one access right of one subject to one resource. Formulate an access matrix and indicates the access rights of a particular subject for a particular object. [Your answers are to be in written form, take photo of your answers, put your answers in MS Word, convert to PDF file and then upload the PDF file. Maximum PDF file size is 1 MB. PDF file name format is "StudentName_QuestionNumber"]



Subject	Access Mode	Object
Bob	Read	1
Bob	Write	1
Bob	Read	2
Bob	Own	4
Bob	Read	4
Bob	Write	4
Alice	Read	1
Alice	Own	2
Alice	Read	2
Alice	Write	2
Alice	Write	3
Alice	Read	4
Darth	Own	1
Darth	Read	1
Darth	Write	1
Darth	Own	3
Darth	Read	3
Darth	Write	3

Table 3: Authorization Table for Files

Add file

b) (iii) Illustrate the TWO (2) directed graphs - "Access Control Lists and Capability Lists" that corresponds to the access matrix which was created / answered by you in Question 4 b) (ii). [Your answers are to be in written form, take photo of your answers, put your answers in MS Word, convert to PDF file and then upload the PDF file. Maximum PDF file size is 1 MB. PDF file name format is "StudentName_QuestionNumber"]

Add file

c) Explain THREE (3) constituents of network security can be used by users to minimize maintenance and improves security. (3

Long answer text Antivirus and anti-spyware, firewall, IDP, VPN

d) Explain THREE (3) strengths of IPsec capability to secure communications across a Local Area Networks, across private and public Wide Area Networks, and across the Internet. (3

Long answer text