Usman Institute of Technology

End-Term Examination Fall 2020 Semester

Course Code: CS413 **Course Title:** Information Security **Date:** 03/03/2021

Maximum Marks: 60 **Max Time Allowed:** 3 hours

PLEASE FILL IN THE FOLLOWING BEFORE PROCEEDING

Seat No. ST-18045 **Roll No.** 18B-129-SE

Batch: 2018 **Enrollment No.** UIT/147/2018-19

Important

This is NOT AN OPEN-BOOK EXAMINATION conducted in line with the online academic policies developed by the NED University of Engineering and Technology. All necessary information about the online examination has been shared with students in advance.

Declaration

I guarantee that all submissions are based on my independent work without any unauthorized help. All activities are completed with full adherence to the "Ethics Policy" of the Institute. I understand that any breach would result in disciplinary action against me as per Institute rules.

☒ I **have read and understood the Students Ethics Policy for Online Assessments.**

(paper will not be graded if the above is not checked)

Note: Submission of this paper certifies that you are agreed to the Students Ethics Policy for Online Assessments and are liable to be judged according to it.

AWARD

		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
Examiner										
ERC										
	Total Marks in Figures				**Total Marks in Words**					

Q1. (a) Generate sub-keys K1 and K2 if the initial key is the (first letter of your name in bits + first bit of this letter and last bit of the letter) in S-DES. **[6]**

(b) After the above process you will have a unique K1 and K2 using this information encrypt the sequence "10110110" (Draw structure of S-DES and traverse the data through it). **[6]**

P10									
3	5	2	7	4	10	1	9	8	6

P4			
2	4	3	1

P8							
6	3	7	4	8	5	10	9

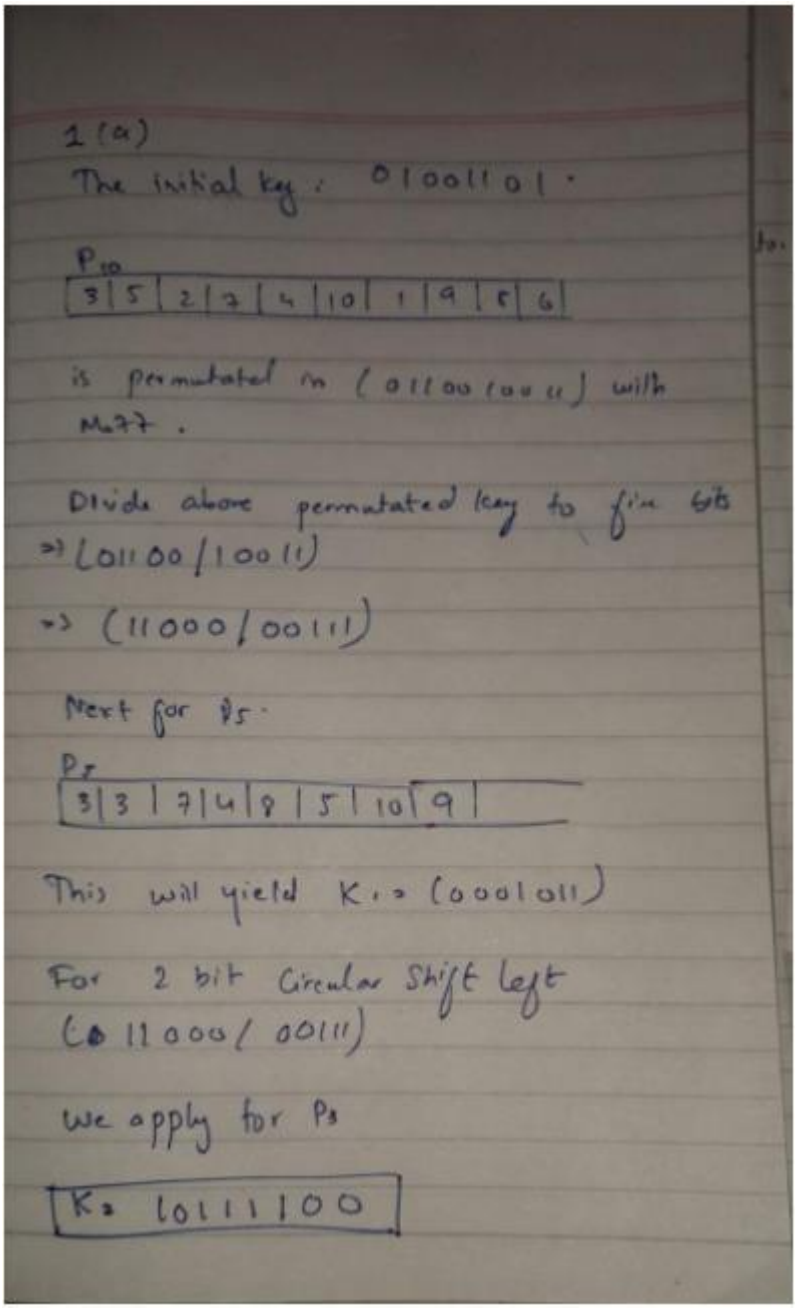
IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

E/P							
4	1	2	3	2	3	4	1

$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array} \qquad S1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

NAME=MANSOOR



Q2. (a) What is "CARE" and how can we utilize this concept to evaluate complex scenarios in Information security ethics. **[4]**

(b) Fahad Khan made a mistake and left his USB at the cafeteria where he works. Later that day while Faraz was having a cup of tea in the cafeteria he spotted the USB. Faraz picked it up with an intention to return it to its owner, later that day Faraz plugged the USB in his laptop to see if the drive is labelled and could give a clue about its owner. After looking at the drive labeled "Fahad Khan" Faraz clicked it to further confirm that he is the same Fahad khan who works in his department in the USB he found several documents and out of curiosity decides to randomly access one of the documents, to his amazement he discovered that it contains names, addresses and NIC numbers this was no ordinary thing it was the payroll information of all the employees, concerned he clicks the readme file that read as follow:

"Saqib look at the files on this disc. Hope they meet your expectations. Wire money

to account as arranged. Rest of data sent on payment."

Faraz further explored the drives and found that credit card numbers and information of family members of each individual is also present in the drive, being information security expert by now it was becoming evident that Fahad khan might be involved with a criminal gang and as an expert is utilizing his efforts to earn money unlawfully. Now Faraz ponders what steps should he take?

Threats and Opportunities:

Following thoughts might be challenging Faraz after disclosure of above information.

1) This is a good opportunity to earn the amount he always wanted so he can buy a house for his family.

2) I can contact Fahad and ask for my share by keeping my mouth shut that way I will earn and will remain safe as well.

3) I have studied and lived until now in accordance to law and ethics I can't do the above deeds.

4) If I complained against him, he might harm me or my family.

5) Should I hack in to his system and observe what else is he doing?

After reading the scenario and thoughts of Faraz you have to apply ACSP (Australasian Council of Security Professionals) also elaborated which actions are most appropriate for faraz so he can remain under the umbrella of ethics. **[8]**

2A

Care is the practice to secure sensitive knowledge obtained in the course of their work duties and should not reveal or exploit it for personal gain to any unwanted group.

Analysis of Case studies using CARE Framework:

C : Consider.

A : Analysis.

R : Review.

E : Evaluate.

The goal of the CARE System is to protect the rights of the stakeholders, which could be the legal, natural or social rights. Their evaluation are made up on the justifications of their actions and reference to the similar occurred events.

Next comes the Review segment, in which we define the civil, natural and social rights of actors and device users and verify whether or not the right is effected and whether or not the CIA of the end-user is directed towards some kind of samples, copies or encrypted communications.

Next comes the analysis portion in which we reverse the positions of the actors in order to verify if any intervention by the actors will have any impact and

Finally, we decide three aspects, whether there is an infringement of the Code of Ethics, whether the acts taken are justified and fair and, finally, we actually apply to a decision taken sometime in the future as the situation occurs.

2B

As per ACSP, after Faraz's conduct, he will have to behave in the interest of his organisation.

Another postulate notes that the act should be in compliance with the statute, which implies that Faraz will have to record the case in accordance with the organisational law.

In addition, because he has access to classified information, he can secure it and prevent forwarding it on to any unauthorised person. He should not even use that information for his personal use or interest as well.

Also, he'd act in such a way that there is no negative impact on the organization as well as other employees working with or associated with Fahad.

He should avoid conflict of interest as well.

He should be objective and truthful while narrating his statement and case.

Lastly, he should be a positive role model for others.

Therefore, he'll definitely go with the third option, that is "I've studied and lived in accordance with law and ethics and can't do above deeds"

Q3. (a) Encrypt M=4 using Rivest Shamir Adleman (RSA) technique and verify your answer by decrypting the result. Value of p & q are 7 and 5 respectively, also discuss what measures you will take if both public and private keys are similar. **[6]**

(b) What are the steps of Information Security Risk Assessment? Elaborate the concept by making ISRA Matrix. **[6]**

3-A:

Ans 3(a)

$M = 4$

$p = 7$

$q = 5$

$n = p \times q$

$\boxed{n = 35}$

$\phi(n) = (7-1)(5-1)$

$\boxed{\phi(n) = 24}$

Now selecting e, $\{1 < e < \phi n\}$ e is CO-PRIME

$\gcd(5, 24) = 1$

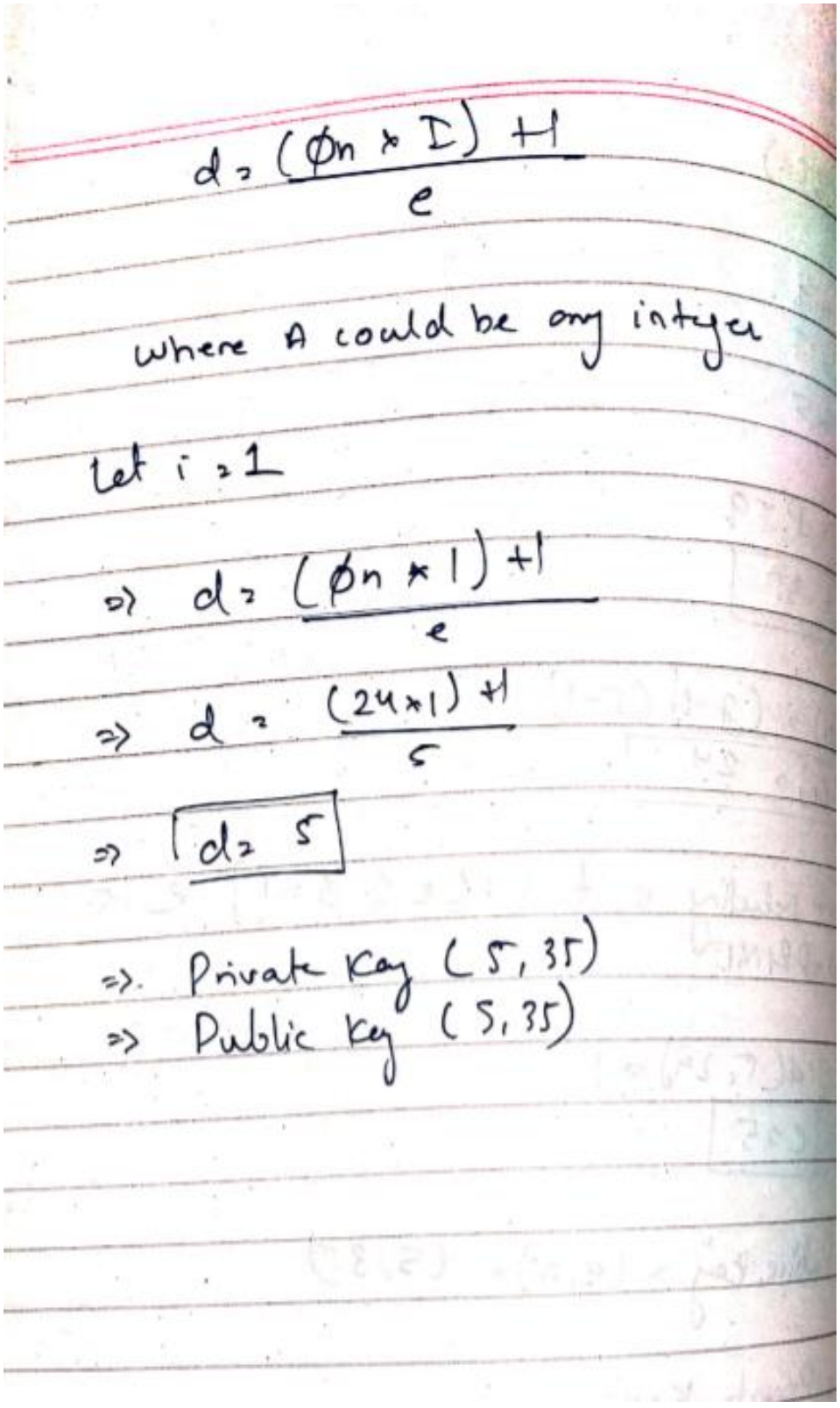
$\boxed{e = 5}$

Public key $= (e, n) = (5, 35)$

For Private Key:

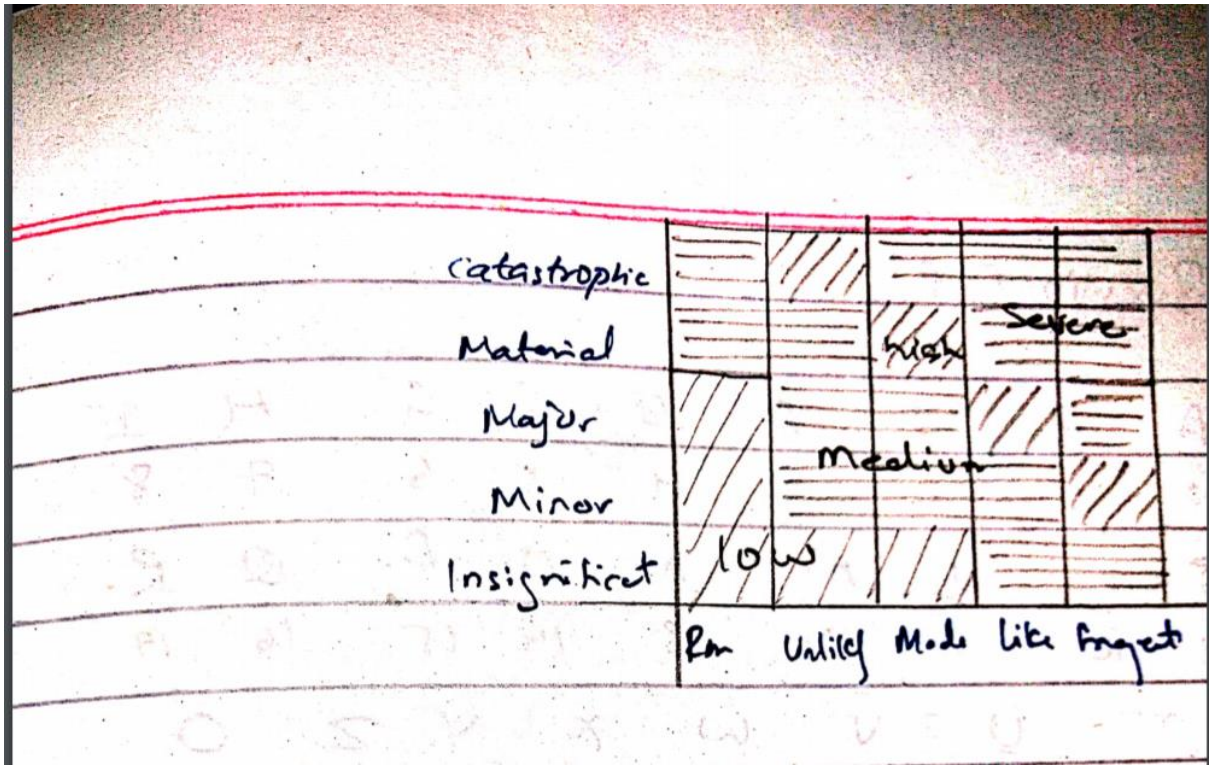
Computing d

$d = e^{-1} \bmod \phi n$



3-B:

The framework of information risk management, risk evaluation lets companies assess and handle events that are likely to affect their confidential data. The method includes finding dangers – whether they be bugs that cyber hackers could hack or errors that workers could make. You then assess the extent of danger that they raise and settle on the appropriate plan of action to prevent them from occurring.



Q4. (a) Utilize the knowledge you gained in class to compress "**/ASK/AS/SKY/SKULL/KU"** using LZW technique, show if compression is possible or not if yes then of how many bits. **[7]**

(b) You are an information security expert and three different organizations have contacted you with their preferences for security implementation. **[3]**

Requirements:

Organization A

Fast Filtering and a single network device could manage it.

Organization B

Should be Resource efficient and checks every session.

Organization C

Should have ability to inspect data characteristics and store network connections.

Suggest the most appropriate firewall to the organizations mentioned above

.

(c) Consider a lab where you are using free space optics for communications, what are the potential possibilities through which eavesdropping can occur? **[2]**

Q4-A

Question 4a

STR = |ASK| AS | SKY | SKULL | KU

Char	StrChar	In table	Output	Add in
/	/			
A	/A	NO	/	256 = /A
S	AS	NO	A	257 = AS
K	SK	NO	S	258 = SK
/	K/	NO	K	259 = K/
A	/A	YES	-	-
S	/AS	NO	/A	260 = /A
/	S/	NO	S	261 = S/
S	/S	NO	/	262 = /S
K	SK	YES	-	-
Y	SKY	NO	SK	263 = SKY
/	Y/	NO	Y/	264 = Y/
S	/S	YES	-	-
K	/SK	NO	/S	265 = /SK
U	KU	No	K	266 = KU
L	UL	NO	U	267 = UL
L	LL	NO	L	268 = LL
/	L/	NO	L	269 = L/
K	/K	NO	/	270 = /K
U	KU	YES	-	-

Q4-B

Association A will have Packet-Filtering Firewall.

Association B will have Circuit-Level-Gateway Firewall.

Association C will have Stateful-Inspection Firewall.

Q5 (a) An employee within your organization used the company's digital camera for business purposes. In the course of doing so, they took a scenic photograph that they then loaded onto

their personal computer by inserting the SD card. The SD card was infected with malware while connected to the employee's personal computer. When re-inserted into a company machine, it infected the organization's system with the same malware. **[3]**

Based on the above scenario, provide answers to the following questions:

1) Who within the organization would you need to notify?

2) How would your organization identify and respond to malware infecting your system through this vector?

3) What other devices could present similar threats?

(b) Make amendments in the conventional Caesar Cipher to encrypt (Your First name + Address), show the changes in the formula. **[Hint** Name: Shamim, Address: A-255 xyz, this will become Shamim255**]** **[4]**

c) Consider Key for Hill Cipher **[5]**

$$K = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

Find K-Inverse to accommodate the Letters, Numbers and Special Characters mentioned below also express the changes in the formula.

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	0	1	2	3
4	5	6	7	8	9	@	#	.	!

5-A

cyber security specialist

They will detect through information leaks and will alter the firewalls.

usb and CD

For the first point, the first and main person to be told will be the boss and the IT specialist in the company, since it is their intellectual commodity that is infected and can create significant chaos in the organisation.

For the second case, the company will first attempt to get the compromised device out of the organization's network, since it is important to keep the virus from spreading deeper through the organization's network and infecting other machines. Then try deleting the malware with a programme or hardware solution.

Such devices other than the sd card are portable storage devices such as USB or external drives or optical drives such as CDs or DVDs, network devices such as switches and servers and other staff machines if the compromised computer is attached to the organization's network.

5-B

Question 5-B:

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8
J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z	O
18	19	20	21	22	23	24	25	26
1	2	3	4	5	6	7	8	9
27	28	29	30	31	32	33	34	35
@	#	.	!					
36	37	38	39					

Name : Mansoor

Add : 40C

=> M → 12

=> (12 + 3) mod 39

=> 15 → P

=> A → 0

=> (0 + 3) MOD 39

=> 3 → D

⇒ N → 13

⇒ (13+3) mod 39

⇒ 16 → Q

⇒ S → 18

⇒ (18+3) mod 39

⇒ 21 → V

⇒ O → 14

⇒ (14+3) mod 39

⇒ 17 → R

⇒ R → 17

⇒ 21 mod 39

⇒ 21 → V

⇒ 4 → 30

⇒ (30+3) mod 39

⇒ 33 → 7

⇒ O → 26

⇒ (26+3) mod 39

⇒ 29 → 3

⇒ C → 2

⇒ 2+3 mod 39

⇒ 5 → F

CIPHER TEXT:

"PDQVRV73F"

5-C