National University of Computer and Emerging Sciences

FAST School of Computing Fall-2023 Islamabad Campus

CS-2005: 3002: Information Security (BS-CS)

Serial No:

Sessional I

Part B

Total Time: 30 min

Total Marks: 30

Monday, 25th September, 2023

Course Instructors

Urooj Ghani, Muhammad Luqman Sumar, Sajid Hussain

____

Signature of Invigilator

________________	__________	__________	______________
Student Name	Roll No.	Course Section	Student Signature

DO NOT OPEN THE QUESTION BOOK OR START UNTIL INSTRUCTED.

Instructions:

1. This is Part B of the final exam; you must have already returned Part A. You MUST write your name and roll number on this page. Please do it now!
2. No additional sheet will be provided for rough work. Use the back of the last page for rough work.
3. If you need more space write on the back side of the paper and clearly mark question and part number etc.
4. After asked to commence the exam, please verify that you have **7** different printed pages including this title page. There are a total of **2** questions.
5. Use permanent ink pens only. Any part done using soft pencil will not be marked and cannot be claimed for rechecking.
6. Calculator sharing is strictly prohibited.
7. You need to be as specific as possible and provide the answers in the space provided. Cutting, overwriting and ambiguous answers would be considered as incorrect.

	Q-1	**Q-2**	**Total**
Marks Obtained			
Total Marks	**20**	**10**	

Question 1 [2*10 = 20 Marks]

Imagine you are a dedicated student who relies on the **SLATE** student portal for managing your academic journey at a prestigious university **FAST NUCES**. **SLATE** is not just a portal; it's your digital campus. However, in recent times, this digital campus has become a battleground for a multitude of security incidents and threats. As you navigate through these challenges, your vigilance and problem-solving skills will be put to the test. Read on to uncover each attack from the description given to you in the form of incident:

Incident	Description	Attack Type
A	It starts innocently enough. You receive an email that appears to be from the **SLATE** portal administration. It's well-crafted, mimicking the university's official communication style. But as you read, an unsettling feeling creeps in. The email demands your personal login credentials, citing an imminent account suspension if you fail to comply. You wonder: is this a genuine request, or is something sinister afoot?	
B	Your phone rings, displaying an unknown number. The voice on the other end claims to be a member of the **SLATE** portal support staff. They sound professional and convincing. They are courteous but insistent, asking for sensitive information like your registration number and **FLEX** credentials under the pretext of resolving a "portal issue." You can't help but question their true intentions.	
C	One morning, as you eagerly log into the **SLATE** portal to check your academic progress, you are met with a horrifying sight. All your academic records and coursework have been encrypted. A menacing message demands payment for the elusive decryption key. Panic sets in as you grapple with the prospect of losing access to your vital academic data.	
D	Navigating through the **SLATE** portal, you encounter a relentless barrage of intrusive advertisements. These ads are obtrusive, irrelevant, and seem unrelated to your academic tasks. They disrupt your study sessions and leave you questioning the integrity of the portal's user experience.	
E	A curious discovery unfolds as you stroll past the recycling bins near the **Margalla Labs**. Among discarded papers and coffee cups, you find printed university documents. Among them, login credentials and sensitive research data are casually strewn about. It's clear that someone may be actively scavenging for discarded information, but their intentions remain a mystery.	

F	On a seemingly secure day, you notice an unfamiliar person trailing closely behind you as you gain entry into the university building. They seem out of place but evade suspicion long enough to slip inside. A sinking feeling tells you that their presence bodes ill for the portal's security.	
G	Users across the portal community report unauthorized access to their **SLATE** portal accounts. Even more distressing, academic records bear the scars of unauthorized changes. It's an academic nightmare that points to a breach - one that may be related to pharming, but nothing is certain.	
H	An unsettling revelation strikes as you attempt to log into your **SLATE** portal account. Your trusted login credentials have inexplicably failed you. Instead, an ominous message appears, demanding a hefty ransom for account restoration. The gravity of the situation hangs heavy on your shoulders.	
I	Amid your portal adventures, you've encountered a web of deceit. Users report that mistyping the **SLATE** portal's web address leads to malicious websites. These deceptive domains are designed to steal your precious login credentials, adding yet another layer of complexity to the security puzzle.	
J	As you explore the **SLATE** student portal, a puzzling situation emerges. There's a challenge that's not like the others, and it involves the FAST NUCES Board of Directors. Instead of traditional attacks, this one is complex. It's like a clever puzzle, where someone is using very tough codes to hide their actions. They're not following the usual rules, making it hard to understand what they're up to. Because of this, it's important to act quickly. Report this strange situation to the "SLATE" portal's IT team and get help from cybersecurity experts. They have the skills to decode this puzzle and make sure the Board of Directors and the portal stay safe from this mysterious attacker. Your academic journey on "SLATE" depends on it.	

Question 2 [10 Marks]

Key (in English): **Thats my Kung Fu**
Translation into Hexadecimal:

T	**h**	**a**	**t**	**s**		**m**	**y**		**K**	**u**	**n**	**g**		**F**	**u**
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

Plaintext (in English): **Two One Nine Two**
Translation into Hexadecimal:

T	**w**	**o**		**O**	**n**	**e**		**N**	**i**	**n**	**e**		**T**	**w**	**o**
54	77	6F	20	4F	6E	65	20	4E	69	6E	65	20	54	77	6F

a. How many rounds are required for AES-128, AES-192 and AES-256 encryption? **(1 Mark)**

b. In AES-128 encryption, how many steps ae involved in the first round and in the last round? Enlist it. **(2 Marks)**

c. Perform the following operations for the provided plaintext block in the first round.

1. Add Round Key **(4 Marks)**

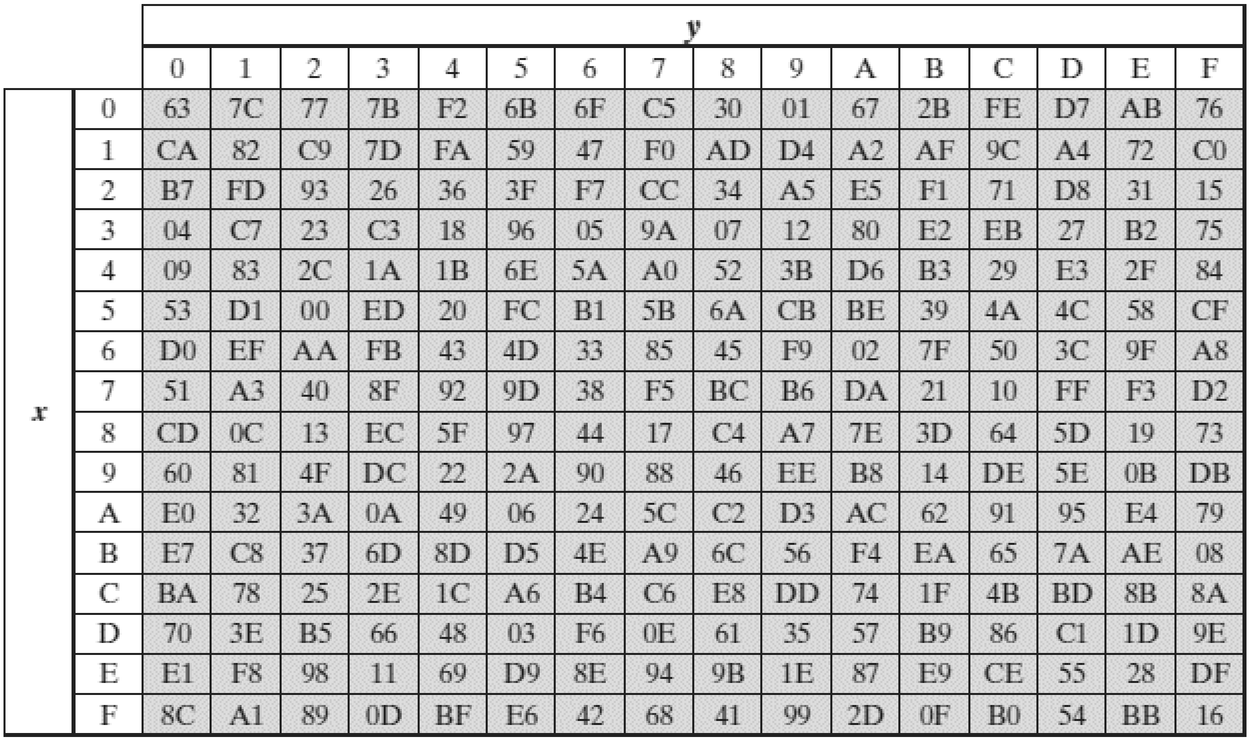
2. Substitute Bytes **(3 Marks)**

Bonus Part ☺

3. Mix Column

Best of Luck ☺

S-box 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

(a) S-box

Constant Matrix

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

Rough Work: