Air University

Mid Examination: Spring 2025

Subjective

(To be solved on Answer Books only)

Subject: Cryptography
Class: F-23
Section(s): A,B
Course Code: CY 212

Time Allowed: 2 Hrs
Max Marks: 50
FM's Name: Jameel Arif
FM's Signature:

INSTRUCTIONS

- Understanding the Question is Part of the Exam
- Attempt responses on the answer book only.
- Nothing is to be written on the question paper.
- Rough work or writing on question paper will be considered as use of unfair means.
- Calculators are allowed.

Q1. **Marks (13) CLO-3**

Question : AES Key Expansion

Task:

- **(1) Draw a flowchart** representing the AES **Key Expansion Algorithm** for generating round keys.
- **(2) Perform step-by-step calculations** to generate the **first-round key** from the given AES-128 initial key.
- **(3)** Present the **flowchart and calculations in parallel**, clearly mapping each step in the algorithm to its corresponding calculation.

pected Answer Format.

- **Left Side:** Flowchart representing **AES Key Expansion** steps.
- **Right Side:** Corresponding **hexadecimal calculations** for each step.

Initial Key: 00010203 03020102 0201020B 0B0203B1

Table 5.2 AES S-Boxes

		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

Rcon Constants (Base 16)			
Round	Constant(Rcon)	Round	Constant(Rcon)
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

Q2. **Marks (12) CLO-1**

Question: Entropy in Information Theory

- **(1)** Provide the **formal definition** of entropy in **Information Theory**, including the **mathematical formula.**
- **(2) Explain,** in simple terms, what entropy represents in the context of information and uncertainty.
- **(3) Calculate the Entropy of the biased coin such that:**
  Head(H): probability = p(H) =0.35
  Tail(T): probability = p(H) =0.65

Using a **step-by-step calculation** to find entropy and interpret the result.

Q3. Marks (12) CLO-2

Question: Create a Comprehensive Flowchart of the DES Encryption Algorithm and Key Scheduling Process

You are required to create a **detailed and well-labeled flowchart** illustrating the **Data Encryption Standard (DES) encryption algorithm** along with its **key scheduling algorithm.** Your flowchart should clearly depict the transformation of the **64-bit plaintext** and the **64-bit key** through the various stages of DES encryption. Each step should be properly labeled with the corresponding **bit size** and **process name** to provide a complete visual representation of the algorithm.

Q4. Marks (13) CLO-2

Question: RSA Encryption – Complex Scenario with a Simple Answer

A company wants to implement **RSA encryption** for securely exchanging messages between two employees: **Alice and Bob**. The company provides the following **RSA parameters:**

- Parameters: **p=3, q=11, ϕ(n)=20, e=3, n=33, d=7**
- Alice wants to send Bob the encrypted message **M** using RSA.

```
If (last_digit_of_your_roll_number_is > 5)
    {M=4;}
else
    {M=3;}
```

- Bob needs to decrypt the received ciphertext **C** to retrieve the original message **M.**

Tasks:

1. **Encryption:** Compute the ciphertext **C.**
2. **Decryption:** Compute the original message **M.**
3. **Answer Format:** Write the **final values** of **C** and **M**, with clear intermediate steps. (please do rough work on a separate sheet)