



School of Computer Science and Engineering

Winter Semester 2023-24

Continuous Assessment Test – I

SLOT E1+TE1

Programme Name & Branch: B.Tech & Computer Science and Engineering

Course Name & Code: Cryptography and Network Security & BCSE309L

Class Number (s): Applicable to all

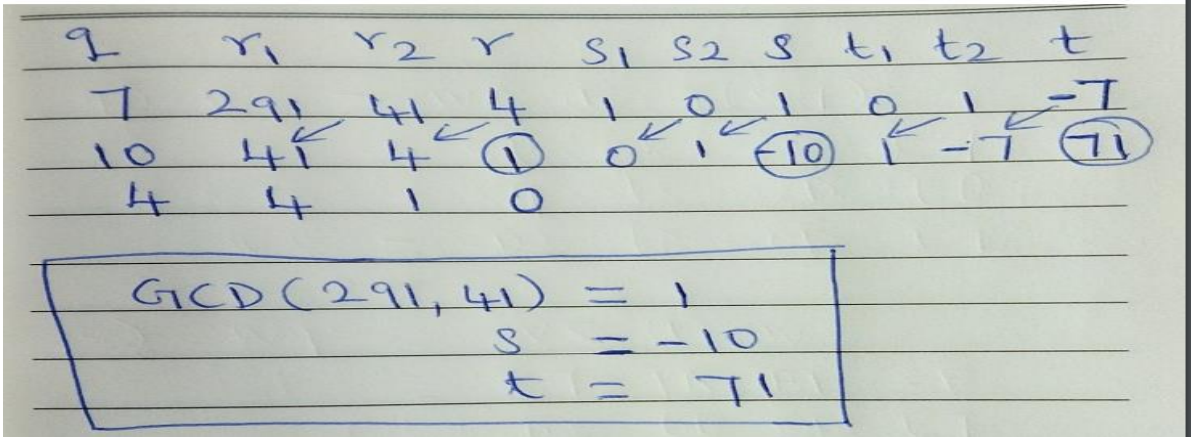
Faculty Name (s): Applicable to all

Exam Duration: 90 Min.

Maximum Marks: 50

General instruction(s):

Answer All the Questions and calculator is allowed

Q. No.	Question	Max Marks
1.	a) Find GCD, variables S and T by construct a table for the following inputs using Extended Euclidean Algorithm. 291, 41.  b) Find the remainder for $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$ using Fermat's Little Theorem. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$. [Solution: $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 0 \bmod 7$] By Fermat's Little Theorem, $2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \bmod 7$. Thus, $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 2^2 + 3^0 + 4^4 + 5^2 + 6^0 \equiv 4 + 1 + 2^8 + 25 + 1 \equiv 4 + 1 + 4 + 4 + 1 \equiv 14 \equiv 0 \bmod 7$.	5

2. A hoard of gold pieces comes into the possession of a band of 15 pirates. When they come to divide up the coins, they find that 3 are left over. Their discussion of what to do with these extra coins becomes animated, and by the time some semblance of order returns there remain only 7 pirates capable of making an effective claim on the hoard. When, however, the hoard is divided between these seven it is found that 2 pieces are left over. There ensues an unfortunate repetition of the earlier disagreement, but this does at least have the consequence that the 4 pirates who remain are able to divide up the hoard evenly between them. What is the minimum number of gold pieces which could have been in the hoard?

$$\begin{aligned}
 x &\equiv 3 \pmod{15} \\
 x &\equiv 2 \pmod{7} \\
 x &\equiv 0 \pmod{4}
 \end{aligned}$$

$\text{GCD}(15, 7)$
 $\text{GCD}(15, 4)$
 $\text{GCD}(7, 4)$
 $= 1$

1) $M = m_1 \times m_2 \times m_3$
 $M = 15 \times 7 \times 4$
 $M = 420$

2) $M_1 = M / m_1$
 $= 420 / 15 = 28$
 $M_2 = 420 / 7 = 60$
 $M_3 = 420 / 4 = 105$

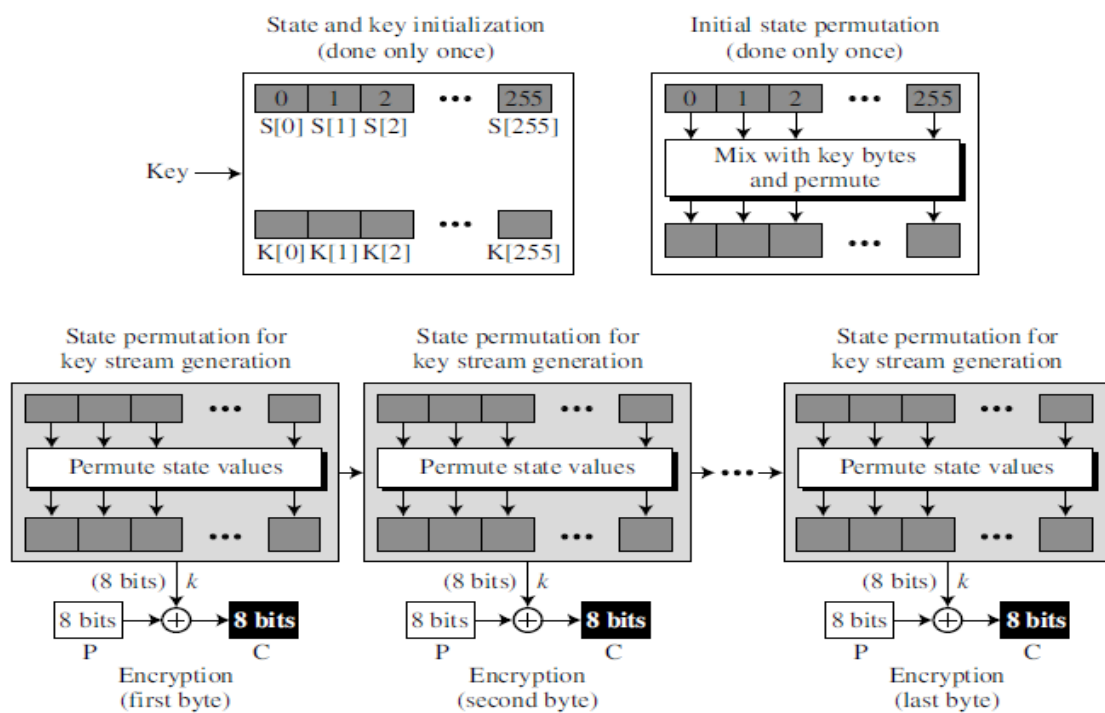
$m_1^{-1} = 28^{-1} \pmod{15}$
 $= 28 \times ? \pmod{15} = 1$
 $= 28 \times 7 \pmod{15} = 1$
 $= 196 \pmod{15} = 1$
 $m_1^{-1} = 7$

$m_2^{-1} = 60^{-1} \pmod{7}$
 $= 60 \times ? \pmod{7} = 1$
 $= 60 \times 2 \pmod{7} = 1$
 $= 120 \pmod{7} = 1$
 $m_2^{-1} = 2$

$$\begin{aligned}
 x &= [(3 \times 28 \times 7) + (2 \times 60 \times 2)] \text{ mod } 420 \\
 x &= [588 + 240] \text{ mod } 420 \\
 x &= 828 \text{ mod } 420 \\
 \boxed{x &= 408}
 \end{aligned}$$

3. Draw an architecture of RC4 algorithm and discuss the process of initialization, initial state permutation, key stream generation and encryption in detail.

10



Architecture – 2
 Initialization process - 2
 Initial state permutation - 2
 Key stream generation - 2
 Encryption - 2

4. a) Explain the DES feistel structure in detail with neat diagram.

5

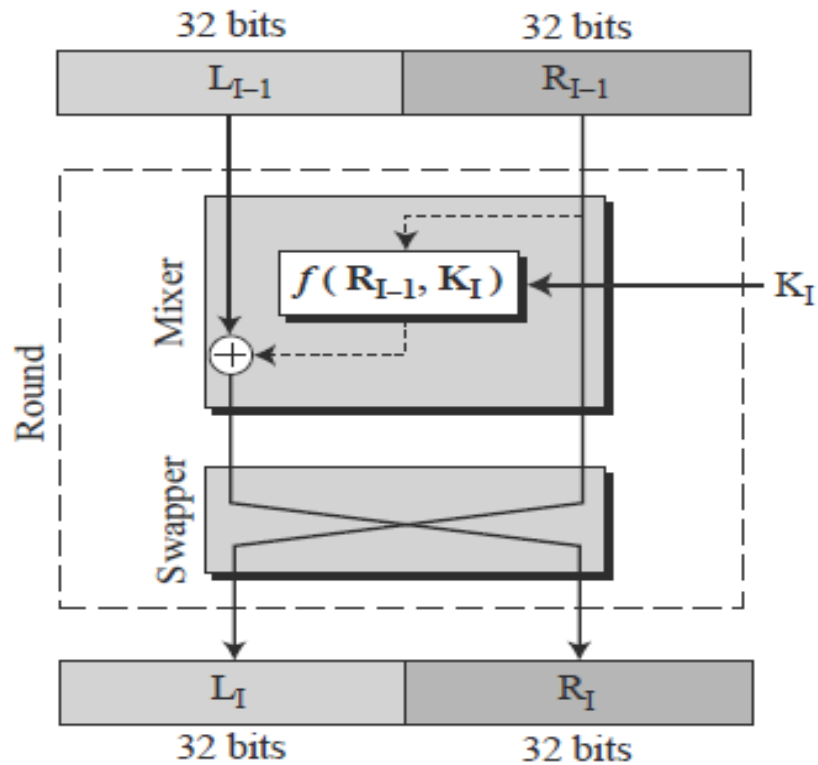


Fig. 6.4 A round in DES (encryption site)

b) Answer the following questions about S-boxes in DES:

- Show the result of passing the input 111111 through S-box 2.
- Show the result of passing the input 000000 through S-box 7.

S-box 2 Table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
1	03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
2	00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
3	13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

S-box 7 Table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	00	08	13	03	12	09	07	05	10	06	01
1	13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
2	01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
3	06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

i)

Input: 1 1111 1 → 3, 15 → Output: 09 (1001)

ii)

Input: 0 0000 0 → 0, 0 → Output: 04 (0100)

5. Find the third round key of AES 128 using the following second round key which is given in hexadecimal, S-Box table and round constant 04.

10

Second Round Key

56	C7	76	A0
08	1A	43	3A
20	B1	55	F7
07	8F	69	FA

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	4D	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

Second Round Key = 56 C7 76 A0
 08 1A 43 3A
 20 B1 55 F7
 07 8F 69 FA
 ↑ ↑ ↑ ↑
 W4 W5 W6 W7

Find

$$g(W7) = g(A0 \ 3A \ F7 \ FA)$$

1) Rotword one byte circular shift
 = 3A F7 FA A0

2) Sub word = 80 68 2D E0

3) EX OR with RC
 = 80 68 2D E0 XOR
 04 00 00 00

$$g(W7) = 84 68 2D E0$$

$$4) W_8 = W_4 \oplus g(W_7)$$

$$= 56 \ 08 \ 20 \ 07$$

$$84 \ 68 \ 2D \ E0$$

$$W_8 = D2 \ 60 \ 0D \ E7$$

$$5) W_9 = W_5 \oplus W_8$$

$$= C7 \ 1A \ B1 \ 8F$$

$$D2 \ 60 \ 0D \ E7$$

$$W_9 = 15 \ 7A \ BC \ 68$$

$$6) W_{10} = W_6 \oplus W_9$$

$$= 76 \ 43 \ 55 \ 69$$

$$15 \ 7A \ BC \ 68$$

$$W_{10} = 63 \ 39 \ E9 \ 01$$

$$\oplus W_{11} = W_7 \oplus W_{10}$$

$$= A0 \ 3A \ F7 \ FA$$

$$\cancel{W_7} \quad 63 \ 39 \ E9 \ 01$$

$$W_{11} = C3 \ 03 \ 1E \ FB$$

Round 3 key:

D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB