Daffodil International University

Department of Software Engineering

Faculty of Science & Information Technology

Final Examination, Fall 2025

Course Code: SE332/SWE322; Course Title: Information System Security/Software Security

Sections & Teachers: (MBH-A, B), (AE-C), (TM-D, E), (AE-F, G, H), (DDK-I)

Time: 2 Hour **Marks: 40**

Answer ALL Questions

[The figures in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

1.

Input value:

Li – 1:

1	1	1	0
1	0	1	0
0	1	0	1
0	0	0	1
0	1	0	0
0	0	1	1
1	1	0	1
0	1	1	0

Ri – 1 :

1 1	1 2	1 3	0 4
1 5	0 6	1 7	0 8
0 9	1 10	0 11	1 12
0 13	0 14	0 15	1 16
0 17	1 18	0 19	0 20
0 21	0 22	1 23	1 24
1 25	1 26	0 27	1 28
0 29	1 30	1 31	0 32

Appendix A: (Only index is given, not value)

9	22	26	14
3	16	21	2
23	32	15	1
28	27	29	7
25	30	24	18
12	13	5	8
17	31	11	20
6	10	4	19

Appendix B: (Only index is given, not value)

19	10	16	4
3	26	21	2
23	11	15	13
8	27	29	7
25	30	24	18
12	1	5	28
17	31	32	20
6	22	14	9

NB: Appendix A for Expansion Permutation and Appendix B for 32 bit Permutation of the output of S-Box.

—Answer all the questions with proper justification.

a)	**Summarize** the issues associated with stream Cipher used in Classical cryptographic algorithms and also demonstrate the process of Single Round of DES proposed by NIST.	[Marks- 5]	CLO-3 *Level-5*
b)	You are given the initial value of 32 bit of Ri-1, Use **Appendix A** to get the index number of 32 bit value of Ri-1 to **determine** the value of 48 bit of Expansion permutation.	[Marks- 4]	
c)	Consider the result of 1(b) as an input for your S-box to **verify** that the output of your S-box is 32-bit when the input is 48 bit. **Note: Use Appendix C for the calculation.**	[Marks- 5]	

	d)	**Determine** the value of Li and Ri. To select the process, the diagram that you presented in the answer of 1(a), will help you. **NOTE:** While using the generated output of S-box to get the value of (Li OR Ri- which one needed), apply **Appendix B** to get the permutation of that 32 bit.	**[Marks- 7]**	
2	*a)*	**Evaluate** the AES encryption process when you have 128 bit of plain text, 192 bit of key size and round key size 4 in words.	[Marks- 4]	CLO-3 *Level-5*
	b)	**Determine** the key value of the 3rd round key from the given value of the 2nd round key using AES key expansion process. **Note: Use Appendix D for the calculation.**	[Marks- 5]	

8C	C9	6D	DF
F4	B9	0C	A7
63	2D	52	1D
15	AA	3F	F2

3. **RSA**: RSA (Rivest–Shamir–Adleman) is one of the most widely used public key cryptographic algorithms. It relies on the mathematical properties of large prime numbers and modular arithmetic. RSA is commonly used for secure data transmission, digital signatures, and key exchange in various cryptographic protocols.

Digital signature: is a cryptographic technique used to verify the authenticity and integrity of digital messages or documents. It involves the use of a mathematical algorithm to generate a unique code, or signature, based on the content of the message and the sender's private key. This signature can then be verified by anyone with access to the sender's public key, ensuring that the message has not been altered and confirming the identity of the sender. Digital signatures are widely used in secure communications, online transactions, and legal documents to provide assurance and security in the digital world.

— Answer all the questions with proper justification.

a)	Using the prime numbers p=17 and q=11, and a public key of 19, **identify** the private key to verify the suitability of your private key and public keys when your message is 2.	[Marks- 5]	CLO-4 *Level-4*
b)	**Illustrate** the working procedure of DSA based digital signature to validate how this process ensures verification and integrity of a message and the owner of the message. Also explain the functional operations of this process.	[Marks- 5]	

Appendix C:

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Appendix D:

X \ Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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	9F
e	F1	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