Daffodil International University

Department of Information Technology & Management

Faculty of Science & Information Technology

Final Examination, Fall 2023

Course Code: ITM 322; Course Title: Software and Web Security

Section: A; Course Teacher: MH

Time: 2 Hours | **Answer All the Questions** | **Marks: 40**

Question 01 *[CO 3, Level 3] [Marks 10]*

Using the following 128-bit produced zero round key i.e. inputted key value from user, **calculate** the key value for the first round key of AES following key expansion process.

38	AA	1D	2F
B9	F2	84	58
27	24	71	A3
18	9F	26	69

Note: Consider the following AES S-Box for your calculation.

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	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

Question 02 *[CO 4, Level 4] [Marks 5+5=10]*

A digital signature uses mathematical techniques to verify the authenticity and integrity of a message, software, or digital document. It creates a unique set of numeric values through specific algorithms, allowing the recipient to identify the source of the message. While the digital signature is private at the start of the data transfer, it becomes public as the transfer progresses.

a. **Detect** the purpose of using Digital Signature. Draw the diagram of the RSA based approach with detailed description.
b. **Illustrate** the detail process of DSA/DSS based Digital Signature with equations and diagram.

Question 03 *[CO 3, Level 3] [Marks 5+5=10]*

The most obvious use of a public key encryption system is to secure communication for privacy. In this system, a sender encrypts a message using the recipient's public key, and only the recipient's corresponding private key can decrypt it.

a. **Construct** a diagram based on the situation provided.
b. The encryption key of a public-key cryptosystem is public and different from the decryption key, which is kept secret (private). You have two prime numbers p = 5 and q = 11, as well as your public key is 19. **Calculate** your private key and encrypted value, justify your answer.

Question 04 *[CO 3, Level 3] [Marks 5+5=10]*

The DES algorithm uses a key of 56-bit size. Using this key, the DES takes a block of 64-bit plain text as input and generates a block of 64-bit cipher text. Please answer the following question.

a. **Detect** the weakness of Classic Cryptographic algorithm. **Explore** how Shanon Feisel proposed the solution to solve the problem. Explain with diagram.

b. NIST implemented the above Shanon Feisel's proposed solution. **Construct** the solution with proper caption.