National University of Computer and Emerging Sciences
Islamabad Campus

0252

Information Security (CS3002) (CS)

Sessional-II Exam

Total Time (Hrs): 1
Total Marks: 55
Total Questions: 4

Date: Nov 4, 2024

Course Instructor(s):
Dr. Sayed Qaiser Ali Shah, Ms. Urooj Ghani,
Mr. Muhammad Aadil Ur Rehman,
Mr. Muhammad Shmayel Ullah
Section(s): (A,B,C,D,E,F,G,H,Y,Z)

Roll No _____ Course Section _____ Student Signature _____

Do not write below this line.

Attempt all the questions.

Instructions:

i. Make sure you have 5 different printed pages
ii. Q3 and Q4.b are to be solved on Answer Sheet provided separately
iii. Solve the remaining questions on Question Paper.

Q1: Sarah and Mike are communicating using Internet for communication. They want to make sure that their communication should not be intercepted by an attacker.

a. They are using Asymmetric encryption, in which each user has two keys i.e. Private Key and Public Keys, which are issued by Certification Authority in the form of Digital Certificate. They want to achieve Confidentiality, Authentication, Integrity and Non-Repudiation using their Private and Public Keys. Suppose Sarah is sending a Message. Fill the blanks on the question paper using the format e.g. Pub-Name and Pri-Name, where Pub is Public Key, Pri is Private key and name is the party name e.g. Mike. **[9 Marks]**

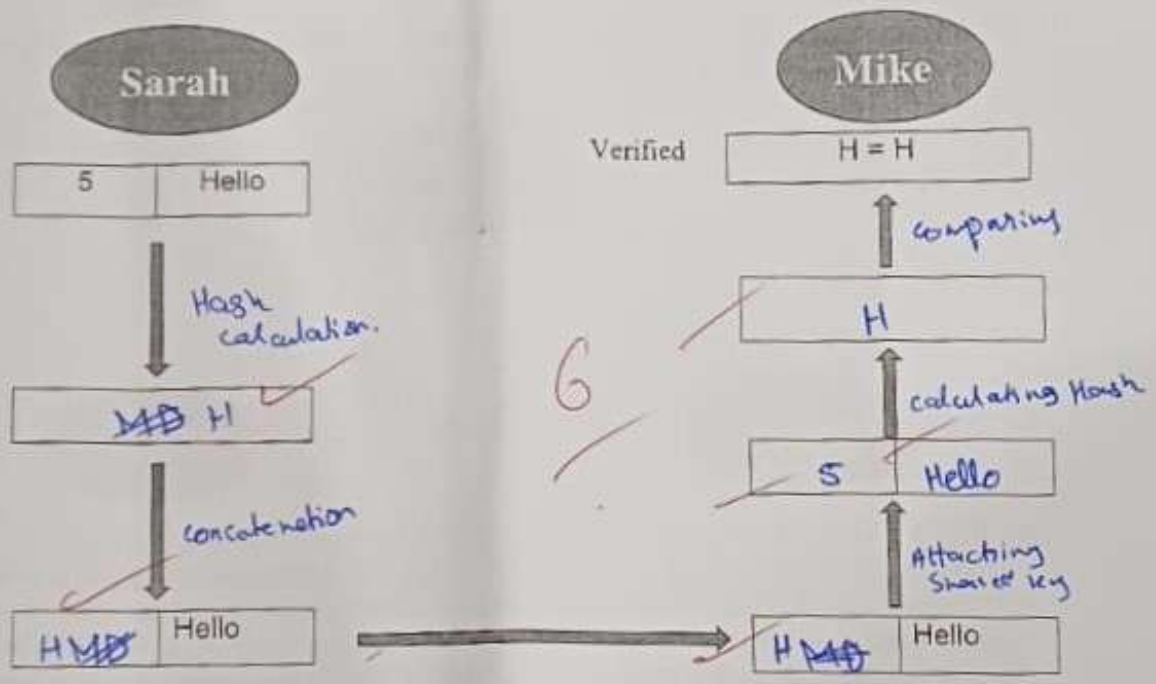
	Encryption	Decryption
Confidentiality	Pub Sarah Mike	Pri Mike
Integrity	H(M) → Pub Mike	Pri Mike
Non-Repudiation	Pri Sarah, Pub Mike	Pri Mike, Pub Sarah
Digital Signature	Pri Sarah	Pub Sarah
Authentication	Pri Sarah, Pub Mike	Pri Mike, Pub Sarah
Digital Certificate	Pri Sarah	Pub Sarah

i. Mike will get Public key of Sarah in a Digital Certificate issued by CA (Certification Authority)

ii. To Achieve Confidentiality and Authentication of a single message it should be encrypted using Pub Mike first and then encrypted using Pri Sarah.

iii. Mike will decrypt the message received from step-ii using Pri Mike first and then Pub Sarah.

b. The Integrity of message can also be achieve using Hashing. Suppose Sarah is sending a message "Hello" and the pre-shared key is 5. How Sarah and Mike will achieve Integrity and Non-Repudiation. You can use Variable "H" for Hashing output. Fill the blanks and make sure that you perform hashing in a correct sequence. **[6 Marks]**



Q2: Alice and Bob wish to communicate securely over an insecure channel. After authentication, they decide to use the Diffie-Hellman key exchange to generate a shared secret key. Here are the details of their setup:

q = Select a value between 13 and 19 (13 < q < 19) **[1 mark]**

α = Select a Smallest Possible Primitive Root **[2 marks]**

XAlice = 4
XBob = 5

Compute the following for Alice and Bob:

Alice	Bob
q = 17	q = 17
α = 3	α = 3
X_{Alice} = 4	X_{Bob} = 5
Y_A = $\alpha^{X_A} \bmod q$ [3 marks] $= 3^4 \bmod 17$ $= 13$	Y_B = $\alpha^{X_B} \bmod q$ [3 marks] $= 3^5 \bmod 17$ $= 5$
K= $(Y_B)^{X_A} \bmod q$ [3 marks] $= (5)^4 \bmod 17$ $= 13$	K= $(Y_A)^{X_B} \bmod q$ [3 marks] $= (13)^5 \bmod 17$ $= 13$

Q3: Encrypt the plaintext "System is hacked" using a columnar transposition cipher. Use the key "SUN". Solve this question in Answer Sheet. **[10 marks]**

Q4: The IT department at FAST NUCES recently discovered a major network security issue. For months, the internet speed on the faculty network had been painfully slow. Upon investigation, they found the surprising culprit: students had been secretly accessing the faculty internet by either guessing weak passwords or bypassing security measures!

This unauthorized access not only slowed down internet speed but also put sensitive faculty data at risk. To address this, the IT team decided to implement a firewall with stronger security protocols to prevent students from accessing restricted networks.

However, just as the firewall was being set up, the system encountered a mysterious encrypted log file titled "Firewall Setup." It seemed like an intruder had left this file as a challenge, and only by decrypting it could the IT team fully restore the network security.

Case Details

File: "**Firewall Setup**"

Encryption Algorithm: AES with a 128-bit key

A cryptic note attached to the file reads:

Message in English: "WiFi is Mine Now"

Message in Hex: 57 69 46 69 20 69 73 20 4D 69 6E 65 20 4E 6F 77 21

W	i	F	i		i	s		M	i	n	e		N	o	w
57	69	46	69	20	69	73	20	4D	69	6E	65	20	4E	6F	77

Key in English: "Catch if U Can:)"

Key in Hex: 43 61 74 63 68 20 69 66 20 55 20 43 61 6E 3A 29

C	a	t	c	h		i	f		U		C	a	n	:	)
43	61	74	63	68	20	69	66	20	55	20	43	61	6E	3A	29

57	20	4D	20
69	69	69	4E
46	73	6E	6F
69	20	65	77

Message Block

43	68	20	61
61	20	55	6E
74	69	20	3A
63	66	43	29

Key Block W3

Using the Mix Columns transformation from the AES algorithm, determine the 2nd byte of the 3rd word of the given message matrix. $(01*20)\oplus(02*4F)\oplus(03*6F)\oplus(01*77)$

a. Write the equation below to find 2nd byte of the 3rd word. **[2 marks]**

$(01*20)\oplus(02*55)\oplus(03*20)\oplus(01*43)$

b. Solve the equation on the Answer sheet and show complete working to find 2nd byte of the 3rd word. **[8 marks]**

c. How many total words are generated after completing the key expansion in AES-128? Use the below table for your Answer. **[2 marks]**

Total Words: 44
How the number you have written above comes? Total 11 keys each key has 4 words so 4x11 = 44 (2)

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Predefined Matrix

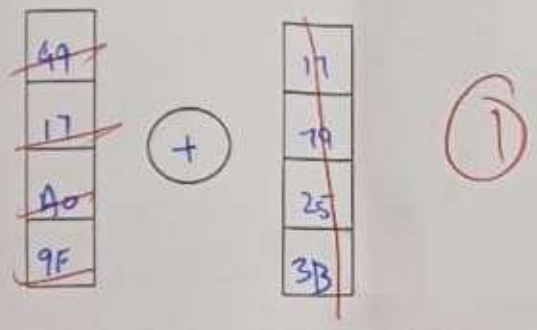
RCON MATRIX									
01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Given the initial key and the expanded words provided in the table below,

43	68	20	61	5F	37	17	56	22	15	49
61	20	55	6E	0C	2C	79	17	1C	30	17
74	69	20	3A	6C	05	25	1F	14	11	A0
63	66	43	29	08	7E	3B	12	85	0B	9F
W0	**W1**	**W2**	**W3**	**W4**	**W5**	**W6**	**W7**	**W8**	**W9**	**W10**

d. Complete the below table to find the values of W11. [3 marks]
Note: DO NOT COMPUTE JUST PUT THE DESIRED VALUES & SYMBOLS.

W11:



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

(a) S-box