Question 1.

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

[Part-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.

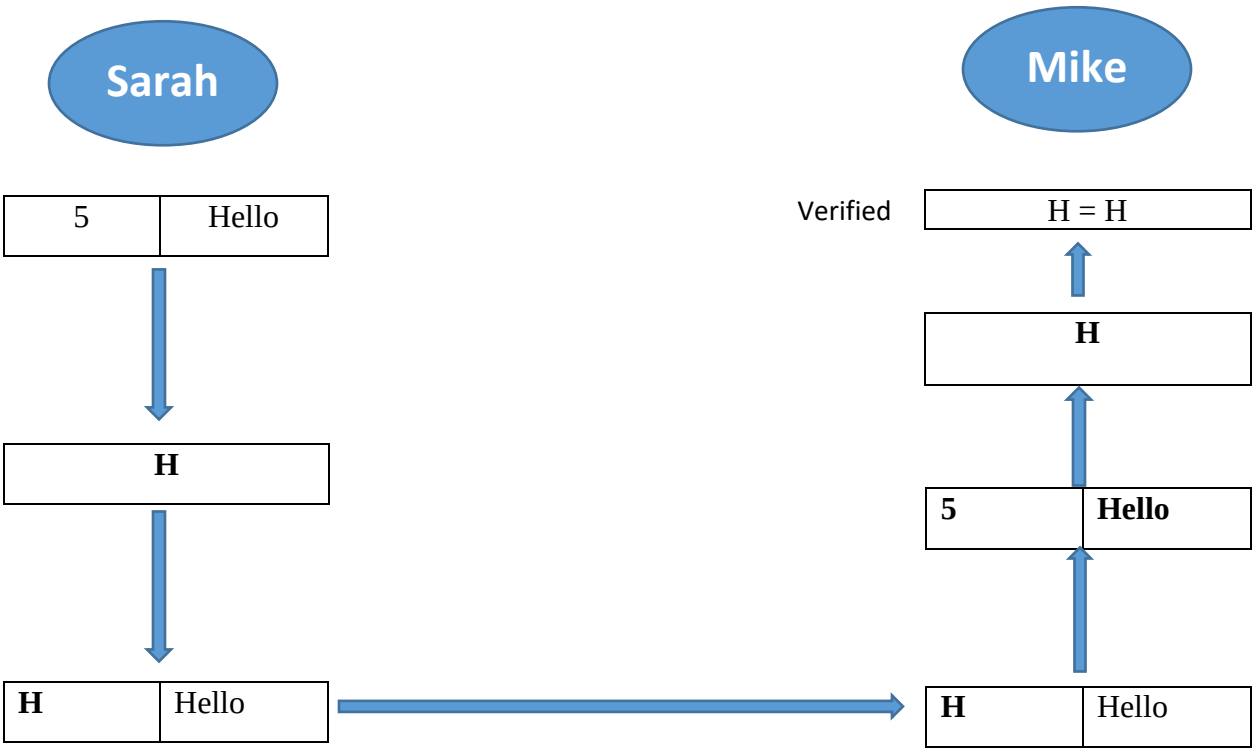
They want to achieve Confidentiality, Authentication, Integrity and Non-Repudiation using their Private and Public Keys. Suppose Sarah is sending a Message. Fill the blanks on the question paper using the format e.g. Pub-Name and Pri-Name, where Pub is Public Key, Pri is Private key and name is the party name e.g. Mike.

	Encryption	Decryption
Confidentiality	Pub-Mike	Pri-Mike
Integrity	Pri-Sarah	Pub-Sarah
Non-Repudiation	Pri-Sarah	Pub-Sarah
Digital Signature	Pri-Sarah	Pub-Sarah
Authentication	Pri-Sarah	Pri-Sarah
Digital Certificate	Pri-Certification Authority	Pub-CA

i. Mike will get Public key of Sarah in a Digital Certificate issued by Certification Authority
ii. To Achieve Confidentiality and Authentication of a single message it should be encrypted using Pri-Sarah first and then encrypted using Pub-Mike
iii. Mike will decrypt the message received from step-ii using Pri-Mike first and then Pub-Sarah .

[Part-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.



Question 2.

Question: 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 = **17** Select a value between 13 and 19 (13 < q < 19) [1 mark]

α = **3** Select Smallest Possible Primitive Root [2 marks]

$X_{Alice} = 4$

$X_{Bob} = 5$

Compute the following for Alice and Bob:

Alice	Bob
q = 17	q = 17
α = 3	α = 3
X_{Alice} = 4	X_{Bob} = 5
$Y_A = \alpha^{X_{Alice}} mod$ q [3 marks for correct answer] = 3^4 mod 17 1 for only formula = 81 mod 17 = 13	$Y_B = \alpha^{X_{Bob}} mod$ q = 3^5 mod 17 = 243 mod 17 = 5
K= $Y_B^{X_{Alice}} \mod q$ $5^4 \mod 17$ $5^4 = 625, \quad 625 \mod 17 = 13$	K= $Y_A^{X_{Bob}} \mod q$ $13^5 \mod 17$ $13^5 = 371293, \quad 371293 \mod 17 = 13$

Question 3. Encrypt the plaintext "System is hacked" using a columnar transposition cipher. Use the key "SUN". Solve this question in Answer Sheet. **[10 marks]**

Follow and fill the Steps as mentioned below.

1. Fill the Grids and assign column order using the key: **(4 marks assigned to the grid on the left side under SUN and 4 marks assigned to the grid on the right side under NSU)**

Key is "SUN", so re-write as rows of 3-letter blocks:

S U N	N S U
2 3 1	1 2 3
S Y S	S S Y
T E M	M T E
I S H	H I S
A C K	K A C
E D X	X E D

2. Highlight columns in the new order and provide the corresponding ciphertext: **(2 numbers for identifying proper ciphertext by writing column wise)**

Corresponding Ciphertext: SMHKXSTIAEYESCD

Another solution if spaces are considered.

Follow and fill the Steps as mentioned below.

1. Fill the Grids and assign column order using the key: **(4 marks assigned to the grid on the left side under SUN and 4 marks assigned to the grid on the right side under NSU)**

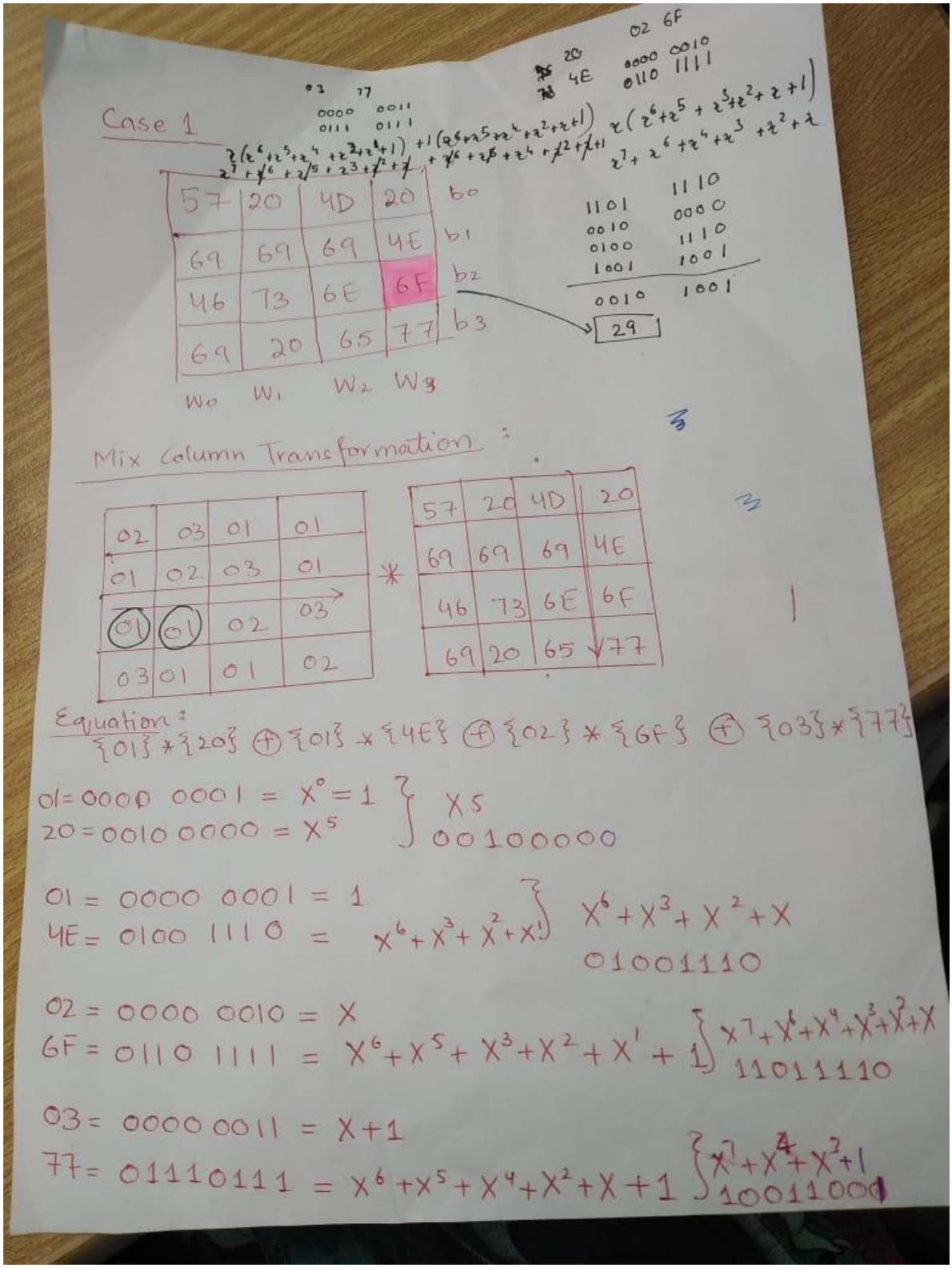
Key is "SUN", so re-write as rows of 3-letter blocks:

S U N	N S U
2 3 1	1 2 3
S Y S	S S Y
T E M	M T E
I S	S I
H A	A H
C K E	E C K
D X X	X D X

2. Highlight columns in the new order and provide the corresponding ciphertext: **(2 numbers for identifying proper ciphertext by writing column wise)**

Corresponding Ciphertext: SMSAEXT CDYEIHKX

Answer 4:


Case 1
57 20 4D 20
69 69 69 4E
46 73 6E 6F
69 20 65 77
b0
b1
b2
b3
W0 W1 W2 W3
1101 1110
0010 0000
0100 1110
1001 1001
0010 1001
29
Mix Column Transformation :
02 03 01 01
01 02 03 01
01 01 02 03
03 01 01 02
Equation :
{01} * {20} ⊕ {01} * {4E} ⊕ {02} * {6F} ⊕ {03} * {77}
01 = 0000 0001 = X^0 = 1
20 = 0010 0000 = X^5
X5
00100000
01 = 0000 0001 = 1
4E = 0100 1110 = X^6 + X^3 + X^2 + X
X^6 + X^3 + X^2 + X
01001110
02 = 0000 0010 = X
6F = 0110 1111 = X^6 + X^5 + X^3 + X^2 + X + 1
X^7 + X^6 + X^5 + X^3 + X^2 + X
11011110
03 = 0000 0011 = X + 1
77 = 01110111 = X^6 + X^5 + X^4 + X^2 + X + 1
X^7 + X^4 + X^3 + 1
10011001

Case 2

57	20	4D	20	b_1
69	69	69	4E	b_2
46	73	6E	6F	b_3
69	20	65	77	b_4
W_1	W_2	W_3	W_4	

0100 1101
0110 0101

1101 0010
1011 0010

~~0110~~ 1000
0100
48

4D
65

02 * 69

0000 0010
0110 1001

$z(z^6+z^5+z^3+1)$

$z^7+z^6+z^4+z$

03 * 6E

0000 0011
0110 1110

$(z^7+z^6+z^4+z^3+z)$
$z^6+z^5+z^3+z^2+z$

Mix Column Transformation:

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

*

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

Equation

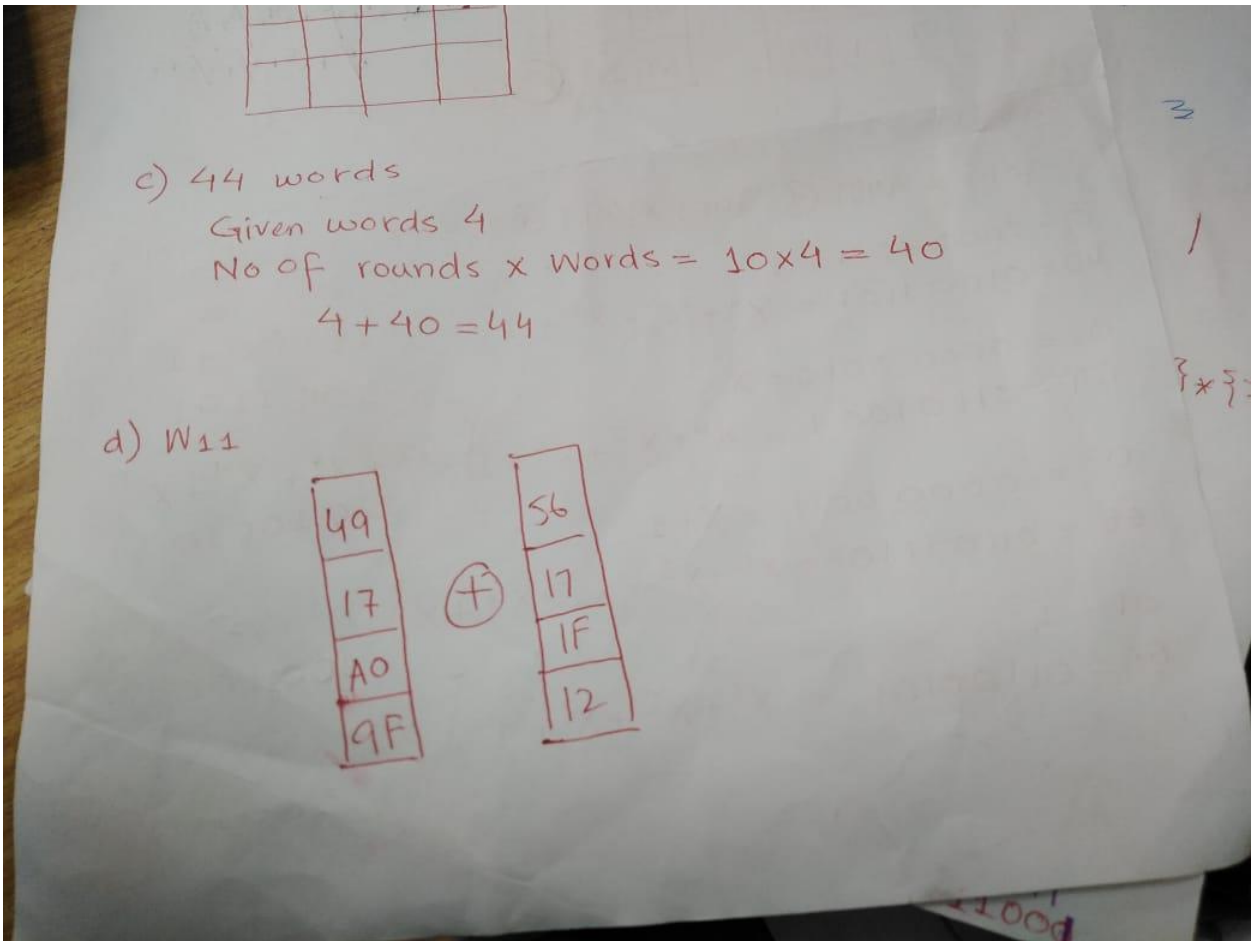
{01} * {4D} ⊕ {02} * {69} ⊕ {03} * {6E} ⊕ {01} * {65}

01 = 0000 0001 = 1
4D = 0100 1101 = $X^6+X^3+X^2+1$ → $X^6+X^3+X^2+1$
01001101

02 = 0000 0010 = X
69 = 01101001 = $X^6+X^5+X^3+1$ → $X^7+X^6+X^4+X$
11010010

03 = 0000 0011 = X+1
6E = 0110 1110 = $X^6+X^5+X^3+X^2+X$ → $X^7+X^5+X^4+X$
10110010

01 = 1
65 = 01100101 = $X^6+X^5+X^2+1$ → $X^6+X^5+X^2+1$
01100101



c) 44 words

Given words 4

No of rounds x Words = $10 \times 4 = 40$

$4 + 40 = 44$

d) W11

49
17
A0
9F

$\oplus$

56
17
1F
12