COLLEGE OF ENGINEERING, PUNE

(An Autonomous Institute of Government of Maharashtra.)

END Semester Examination

Programme: B.Tech | **Semester: VII**

Course Code: CT-18002 | **Course Name: Cryptography and Network Security**

Branch: Computer Engineering | **Academic Year: 2019-20**

Duration: 3 hrs | **Max Marks: 60**

Student PRN No.

1	1	1	6	0	3	0	6	7

Instructions:

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Writing anything on question paper is not allowed.
4. Exchange/Sharing of stationery, calculator etc. not allowed.
5. Write your PRN Number on Question Paper.

			Marks	CO	PO
Q 1	a	Define the following terms: (i) Keyspace (ii) Confusion	[2]	1	1
	b	Suppose the key matrix for Playfair Cipher is as given below	[4]	1	1

B	O	V	P	U	E
6	5	H	A	I	0
R	W	2	Q	G	7
I	C	X	K	L	9
4	S	M	Y	D	J
N	3	F	8	T	Z

The message is: "Meet me in Pasadena, CA at 1 pm on 7 October."

What is the ciphertext?

	c	We will use the standard 26-letter English alphabet, with three more characters "?" (Question mark), "." (Full stop), and "_" (underscore) appended to the end as shown below.	[4]	1	1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

The key for encryption is CDEF. Using Hill cipher for encryption, the ciphertext generated is:

COEP_PUNE.WHERE?

Find the plaintext.

Q 2 **a** Compute GCD (354448, 233456)? [3] 2 1

b Calculate $\Phi(529)$. [2] 2 1

c Compute the last two digits of 49^{19} using Chinese Remainder Theorem. [4] 2 1

d Consider the following S-Box for the DES algorithm. Given input $(000110)_2$, the output of the S-Box is:---------- [1] 3 4

S-Box

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

Q 3 **a** Draw a block diagram for the first round of DES algorithm. [3] 1 4

b List the different parameters used in the design of Feistel structure. [2] 1 1

c The key for AES algorithm in hexadecimal is as given below: [5] 1 4
54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Generate the subkey for the first round of AES encryption.

S-Box

	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

Q 4 a Consider the RSA cryptosystem with the public parameters, [4] 1 4

$n = 4003997$ and $e = 379$.

Assume you know that $\Phi(n) = 3999996$.

a) Find the decryption exponent d.

b) Find p and q such that $n = pq$

b Write a Diffie-Hellman key exchange algorithm. Explain the procedure for selecting the various parameters in the algorithm. [3] 1 4

c What is the size of hash/ message digest and the block for Secure Hash Algorithm? If the size of message is 514 bits, how many numbers of bits are required for padding this message? Justify your answer. [3] 3 4

Q 5 Attempt **Any Two** of the following questions.

a Write the following algorithms for digital signature schemes: [5] 1 3

(i) A key generation algorithm

(ii) A signing algorithm

(iii) A verification algorithm

b Explain the working of Record protocol in Secure Socket Layer (SSL). [5] 3 1

c Explain the various fields of X.509 Certificates. Why is Certificate Hierarchy required? [5] 1 3

Q 6 Attempt **Any Two** of the following questions.

a What is Intrusion Detection System? List different types of IDS. List and explain various types of Intruders. [5] 4 5

b Explain packet filtering firewall with its advantages and disadvantages. [5] 4 5

c What are the different types of DNS protocol attacks? Explain each in details. [5] 3 1