No. of Printed Pages : 4

M00925 **MMTE-006**

M.Sc. (MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE) M.Sc. (MACS)

Term-End Examination,

December 2019

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours] *[Maximum Marks : 50*

*Note : Answer **any four** questions out of questions No. 2 to 6. Questions No. 1 is **compulsory**. Calculators are **not** allowed.*

1. Which of the following statements are true and which are false? Give proper justification for your answers. 10

i) There is only one kind of polynomial time algorithm for Primality testing.

ii) $(x^2 - 3)$ is an irreducible polynomial over every field.

iii) A Linear Feedback Shift Register (LFSR) always generates a random sequence.

iv) According to the birthday paradox, given a group of 70 people and a fixed date, there will be at least two people from this group having their birthday on this date.

v) The encryption exponent of the RSA algorithm is always odd.

2. a) Find the greatest common divisor h(x) of the polynomials (x^4+3) and (x^6+x^3+2x+1) over $\mathbb{Z}_5\ [x]$. Also find Q (x) and R (x) such that Q (x) (x^4+3) + R (x) (x^6+x^3+2x+1) = h (x). 7

   b) Draw a schematic diagram for the feed back shift register with characteristic polynomial $x^3 + x + 1$. 3

3. a) Encrypt the following text using the columnar transposition with column width 5. 4

   AVIATION is A CHALLENGING PROFESSION. What will be corresponding cipher if one uses (4, 3, 1, 2, 5) as key for shuffling columns?

   b) Check whether 2 is a generator of $\mathbb{Z}_{11}^*$. If yes, calculate the 'Discrete log of 7 base 2' over $\mathbb{Z}_{11}$. Otherwise obtain a generator for $\mathbb{Z}_{11}^*$. 3

   c) What is the little-endian format in data representation? How will the word A : 37262301 be represented in this format? 3

4. a) Determine order of all elements of $\mathbb{Z}_{14}^*$ is it a cyclic group? If so, why? If not, why not? 5

   b) In an RSA cryptosystem, let n = 55 and e = 27. If the ciphertext under this system is 23, find the plaintext. 5

5. a) Find approximate number of primes less than 1000. (Take log 10 = 2.30) 2

b) The round key of AES is 10 35 ed ac ff 60 77 85 bf ca 5d 76 32 cc f4 21. 8

Apply one round of AES to find the ciphertext of the following plaintext :

aa cb 34 fd 57 cd 25 37 92 ee 28 65 ac e3 3f 88.

(The S-box of AES is given below)

	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	F3	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	19	96	05	9A	07	12	80	E2	EB	27	E2	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	81	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	8F	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	BB	BA
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

6. a) i) Yasmin sets up an Elgamal cryptosystem with parameters p = 173, g = 2 and x = 3. What information does she need to make public?

ii) If Zora wants to send the message M = 21 to Yasmin, and chooses k = 5, what ciphertext does she need to send to Yasmin?

iii) If Yasmin receives the ciphertext (8, 54) from another friend, Shiva, then 'what is the plaintext she has received? 5

b) Check whether or not the following sequence passes the poker test, with level of significance $\alpha = 0.05$. 5

1101 0101 1111 0011 0010 1001 1011 0001 1110 1101 0100 1001.

[The following values may be of use to you :

$\chi^2_{0.5,3} = 2.36597$,

$\chi^2_{0.05,1} = 3.84146$,

$\chi^2_{0.05,3} = 7.81473$]

✧✧✧✧✧✧