No. of Printed Pages : 4

MMTE-006

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

Term-End Examination

December, 2020

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

Note : *(i) Answer any* ***four*** *questions from question nos.* ***1*** *to* ***5****.*

(ii) Question ***No. 6*** *is compulsory.*

(iii) Calculator is ***not*** *allowed.*

1. (a) Encrypt the plain text : 4

"They alone live who live for others"

using the Vigenire cipher with the key "IGNOU"

(b) Give any ***two*** cryptographic applications of hash functions. 2

(c) Alia and Bimal decide the use of Diffie-Hellman key exchange, with $p = 41$ and $q = 7$. Alia chooses $a = 3$, and Bimal chooses $b = 4$. What is the key ? 4

2. (a) Explain the Runs test for random sequences. Apply the test for the following sequence : 5

10111	00001	10111	01001	01101	10110	10100	10101
00110	01001	10001	10011	11101	10111	11110	10110
11010	11100	10011	11001	10001	11000	10100	10010
11010	10100	10110	10111	10110	11011	01001	11010

You may like to use the following values :

$\chi^2_{0.05,3} = 7.8147$, $\chi^2_{0.05,4} = 9.48773$, $\chi^2_{0.05,5} = 11.0705$

(b) Factorise 616, using the Fermat factorisation method. 2

(c) Use the repeated squaring method to find $7^5 \pmod{23}$. 3

3. (a) Using the intended Euclidean algorithm, compute $357^{-1} \pmod{1234}$. 5

(b) Sonu wants to use the digital signature algorithm. She chooses $p = 23$, $q = 11$, $g = 2$ and $a = 3$.

(i) What information does Sonu need to make public ? $1\frac{1}{2}$

(ii) She chooses the secret value $k = 5$. Calculate the digital signature of message M = 13, showing all the steps used in the process. $3\frac{1}{2}$

4. (a) Construct a finite field of order 9. Write down the multiplication table of the field. 6

   (b) Decrypt the message $c = 12$ that was encrypted using the RSA algorithm with $e = 7$ and $n = 33$. 4

5. (a) Suppose that we have the following 128-bit AES key, given in hexadecimal form : 5

   1 2 3 4 5 6 7 8 9 0 A B C D E F 1 F E D C B A 9 8 7 6 5 4 3 2 1

   Construct the next 128-bit round key using key scheduling algorithm. Use the table below :

		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
Y	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

   (b) Check whether or not 65 is a composite number, using the Miller-Robin test. 5

6. Which of the following statements are true ? Give reasons for your answers. 10

(i) Every pseudo-random sequence is a random sequence.

(ii) In the DES algorithm, the 64-bit key input is shortened to 56 bits.

(iii) The characteristic of a field is the number of elements in it.

(iv) The probability of choosing a number x, $1 \leq x \leq pq^{-1}$, such that $\gcd(x, pq) \neq 1$ is $\frac{1}{p} + \frac{1}{q}$, where p and q are distinct primes.

(v) The cipher text of the plain text "INDIA", by using the Caesar cipher, is "KPFKC".