MIS No. [ ][ ][ ][ ][ ][ ][ ][ ]

COLLEGE OF ENGINEERING, PUNE
(An Autonomous Institute of Government of Maharashtra.)
SHIVAJI NAGAR, PUNE - 411 005
Department of Computer Engineering and IT

B. Tech. [Computer Engineering]
Subject:- Cryptography and Network Security
Test - II

Max. Marks: 20
Time: 1 Hr. Date: 21/10/2018

Instructions:

1. Figures to the right indicate the full marks.
2. Mobile phones and programmable calculators are strictly prohibited.
3. Exchange/Sharing of anything like stationery, calculator is not allowed.
4. Show your work for all questions

Q.1. **(a)** List the steps in sequence for the key generation process of Advanced Encryption Standard. The key in Hex for AES encryption is as given below: **[4]**

54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

Derive the subkey for first round of encryption.

(b) How many blocks are affected if there is an transmission error in the n^{th} block of ciphertext in ECB and CBC modes? **[2]**

(c) Describe how DES and AES provide confusion and diffusion. **[2]**

(d) In which mode of operation is the initialization vector (IV) used. Give the importance of initialization vector (IV) in modes of operation. **[2]**

Q.2. **(a)** Factor the RSA number n = 3844384501 using the knowledge that **[3]**

$3117761185^2 = 1 \pmod{3844384501}$.

Show your all steps of the calculation.

(b) User A chooses simplified IDEA encryption technique with key **[4]** 1100 0110 0011 0101 1111 0111 0101 1010. Generate all the subkeys required for decryption.

(c) Find the smallest but greater than 2, primitive root of 13? Justify your answer. **[3]**

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