K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June 2024
(B.Tech / M.Tech.) Program: Computer Engineering Scheme :II
Regular Examination: TY Semester: VI
Course Code: CEC602 and Course Name: Cryptography and System Security
Date of Exam: Duration: 2.5 Hours Max. Marks: 60

Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.

		Max. Marks	CO	BT level
Q 1	Solve any six questions out of eight:	12		
i)	Calculate $\phi(240)$	2	1	Ap
ii)	Explain electronic code block mode of operation	2	2	U
iii)	Explain Cryptographic hash function	2	3	U
iv)	Explain User authentication	2	4	U
v)	Compare Dos and DDos	2	5	U
vi)	Explain SQL injection with an example.	2	6	U
vii)	Enlist components of Public Key Infrastructure	2	2	U
vii)	Explain what is Packet sniffing.	2	5	U
Q.2	Solve any four questions out of six.	16		
i)	Calculate the smallest positive residue y in following congruence 7^69= y mod 23	4	1	Ap
ii)	Calculate following A) If user A has private key XA=10 ,what is A's public key YA? B) If user B has private key XB=24,what is B's public key YB? C) What is the shared secret key? User A and B use the Diffie Hellman key exchange technique.They agree with common prime n=67 and a primitive root g=5.	4	2	Ap

K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June 2024
(B.Tech / M.Tech.) Program: Computer Engineering Scheme :II
Regular Examination: TY Semester: VI
Course Code: CEC602 and Course Name: Cryptography and System Security
Date of Exam: Duration: 2.5 Hours Max. Marks: 60

iii)	Explain Properties of secure hash function	4	3	U
iv)	Compare digital signature and digital certificate	4	4	U
v)	Explain ARP Spoofing with its defense measure	4	5	U
vi)	Compare Virus and Worms	4	6	U
Q.3	Solve any two questions out of three.	16		
i)	Find integers p and q such that 51p+36q=3.Also find the GCD of (51,36)	8	1	AP
ii)	Explain various different types of Challenge based response.	8	4	U
iii)	How is security achieved in Transport and Tunnel modes of IPSEC ? Explain AH and ESP	8	5	U
Q.4	Solve any two questions out of three.	16		
i)	Generate the subkey for first round of the AES algorithm.The key in hexadecimal is: 64 46 5a 65 82 ab 7c 73 4e 5b 47 5b 47 8d 9a 12 35 57 Find out g(w[3]) **Given:** S Box	8	2	Ap

x \ y	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

May-June 2024
(B.Tech / M.Tech.) Program: Computer Engineering Scheme :II
Regular Examination: TY Semester: VI
Course Code: CEC602 and Course Name: Cryptography and System Security
Date of Exam: Duration: 2.5 Hours Max. Marks: 60

	Inverse S Box y x 0 1 2 3 4 5 6 7 8 9 a b c d e f 0 52 09 6a d5 30 36 a5 38 bf 40 a3 9e 81 f3 d7 fb 1 7c e3 39 82 9b 2f ff 87 34 8e 43 44 c4 de e9 cb 2 54 7b 94 32 a6 c2 23 3d ee 4c 95 0b 42 fa c3 4e 3 08 2e a1 66 28 d9 24 b2 76 5b a2 49 6d 8b d1 25 4 72 f8 f6 64 86 68 98 16 d4 a4 5c cc 5d 65 b6 92 5 6c 70 48 50 fd ed b9 da 5e 15 46 57 a7 8d 9d 84 6 90 d8 ab 00 8c bc d3 0a f7 e4 58 05 b8 b3 45 06 7 d0 2c 1e 8f ca 3f 0f 02 c1 af bd 03 01 13 8a 6b 8 3a 91 11 41 4f 67 dc ea 97 f2 cf ce f0 b4 e6 73 9 96 ac 74 22 e7 ad 35 85 e2 f9 37 e8 1c 75 df 6e a 47 f1 1a 71 1d 29 c5 89 6f b7 62 0e aa 18 be 1b b fc 56 3e 4b c6 d2 79 20 9a db c0 fe 78 cd 5a f4 c 1f dd a8 33 88 07 c7 31 b1 12 10 59 27 80 ec 5f d 60 51 7f a9 19 b5 4a 0d 2d e5 7a 9f 93 c9 9c ef e a0 e0 3b 4d ae 2a f5 b0 c8 eb bb 3c 83 53 99 61 f 17 2b 04 7e ba 77 d6 26 e1 69 14 63 55 21 0c 7d			
ii)	Explain step by step working of SHA-1 algorithm	8	3	U
iii)	Explain causes of Buffer overflow and what are the prevention measures with examples.	8	6	U

****