M.Tech Odd Semester (CBCS) Exam., December—2017

COMPUTER SCIENCE AND ENGINEERING

(1st Semester)

Course No. : MCSEEL–01/MCSEEL–24

Full Marks : 50
Pass Marks : 15

Time : 2 hours

Note : 1. Attempt *any* **five** questions.
2. Begin each answer in a new page.
3. Answer parts of a question at a place.
4. Assume reasonable data wherever required.
5. The figures in the margin indicate full marks for the questions.

Course No. : MCSEEL–01

(Cryptography and Information Security)

1. *(a)* Encrypt the plaintext "HELLO" using Playfair cipher with the following key : 4

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

(b) For Vigenere cipher, find the ciphertext of a message "She is listening" using the keyword "PASCAL". 6

2. *(a)* Consider a 256-bit AES cryptosystem. Explain the substitution and shift rows operations performed in after the first round key has been added. 5

(b) Explain the encryption technique in cipher feedback mode (CFB). Mention the advantage and disadvantage of CFB. 5

3. *(a)* Why are asymmetric cryptosystems more useful than symmetric cryptosystems? 2

(b) How are encryption and decryption performed in RSA? Write the algorithm for fast computation of modular exponentiation used in RSA. 8

4. *(a)* What is trapdoor one-way function? Why is it used in asymmetric cryptosystem? 2

(b) Write the Diffie-Hellman key exchange protocol. How is this protocol vulnerable to man-in-the-middle attack? 5+3=8

5. *(a)* Define a session key. How can a KDC create a session key between Alice and Bob? 5

(b) Define Kerberos and name its servers. Briefly explain the duties of each server. 5

6. Compare and contrast a conventional signature from a digital signature. Explain arbitrated digital signature. Differentiate between direct and arbitrated digital signature. 2+5+3=10

7. Define Pretty Good Privacy (PGP). What are the five principal services provided by PGP? Why does PGP generate a signature before applying compression? 2+5+3=10

8. Explain the working principle of proxy server. Mention the prime disadvantage of it. What are the attacks that can be made on packet-filtering routers firewall? 4+2+4=10

Course No. : MCSEEL–24

(Theory of Computation)

1. Define and explain Turing recognizable and Turing decidable language. Prove that the language A_{DFA} is decidable. 4+6=10

2. Define deterministic Turing machine and non-deterministic Turing machine. Prove that every non-deterministic Turing machine has an equivalent deterministic Turing machine. 3+7=10

3. Define Post Correspondence Problem (PCP) and Modified Post Correspondence Problem (MPCP). Prove that MPCP is mapping reducible to PCP. 3+7=10

4. Prove that 3-satisfiable is NP-hard by constructing a polynomial-time reduction of S_{AT} to it. 10

5. (a) Define mapping reducible. Prove that if A is mapping reducible to B and B is decidable, then A is decidable. 1½+3½=5

(b) Prove that R is uncountable. 5

6. Define the following : 2×5=10

(a) Polynomial time verifier

(b) TIME $(t(n))$

(c) NTIME $(t(n))$

(d) NP complete

(e) Space complexity

7. Define linear bounded automata (LBA). Prove that A_{LBA} is decidable. 10

8. Prove that every $t(n)$ time multitape Turing machine has an equivalent $0(t^2(n))$ time single-tape Turing machine. 10

★ ★ ★