

Roll No.

Total No. of Pages : 02

Total No. of Questions : 09

B.Tech.(IT) (2012 to 2017) (Sem.-6)

INFORMATION SECURITY AND RISK MANAGEMENT

Subject Code : BTIT-602

M.Code : 71172

Time : 3 Hrs.

Max. Marks : 60

INSTRUCTION TO CANDIDATES :

1. SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.
2. SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.
3. SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.

SECTION-A

Q1) Answer briefly :

- a) What is a one way function?
- b) Name three broad categories of applications of public key cryptosystem.
- c) What are key principles of security?
- d) What is a public key certificate?
- e) What are the properties a digital signature should have?
- f) Why does PGP generate a signature before applying compression?
- g) What protocols comprise SSL?
- h) What is threat assessment?
- i) What is Information Security Life Cycle?
- j) What are IPSec protocols?

SECTION-B

- Q2) Using $e = 13$, $d = 37$, and $n = 77$ in the RSA algorithm, encrypt the message “GOOD” using the values of 00 to 25 for letters A to Z. For simplicity, do the encryption and decryption character by character.
- Q3) What requirements must a public-key cryptosystem fulfill to be a secure algorithm?
- Q4) What is message Integrity? What are the different ways of preserving the integrity of a document?
- Q5) What are various types of malicious programs? Explain various types of Viruses.
- Q6) Comment on the differences between MD4 and MD5. Specifically, to what extent do you think that MD5 is stronger than MD4, and why?

SECTION-C

- Q7) In Secure Socket Layer (SSL) and Transport Layer Security (TLS), why is there a separate Change Cipher Spec Protocol, rather than including a change_cipher_spec message in the Handshake Protocol?
- Q8) What is message authentication? What types of attacks are addressed by message authentication? List some approaches to producing message authentication. In what ways can a hash value be secured so as to provide message authentication?
- Q9) Explain various modes of Risk Analysis.

NOTE : Disclosure of identity by writing mobile number or making passing request on any page of Answer sheet will lead to UMC against the Student.