Code No: 126AQ

R13

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, December - 2018
INFORMATION SECURITY
(Computer Science and Engineering)

Time: 3hours　　　　　　　　　　　　　　　　　　　　　　　　**Max.Marks:75**

Note: This question paper contains two parts A and B.
　　　　Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B
　　　　consists of 5 Units. Answer any one full question from each unit. Each question carries
　　　　10 marks and may have a, b, c as sub questions.

PART- A

(25 Marks)

1.a)　Compare transposition ciphers with substitution cipher.　　　　　　　　　　　[2]
　b)　Explain the principles of security.　　　　　　　　　　　　　　　　　　　　[3]
　c)　What are the advantages of public key cryptography algorithm comparing ryman
　　　encryption algorithm.　　　　　　　　　　　　　　　　　　　　　　　　　[2]
　d)　List the advantages of elliptic-curve cryptography.　　　　　　　　　　　　[3]
　e)　List three approaches to message authentication.　　　　　　　　　　　　　[2]
　f)　What is the function of TGS server in Kerberoes.　　　　　　　　　　　　　[3]
　g)　What are S/MIME message?　　　　　　　　　　　　　　　　　　　　　　[2]
　h)　List the different encryption and authentication algorithms used for AH and ESP
　　　protocols.　　　　　　　　　　　　　　　　　　　　　　　　　　　　　[3]
　i)　What are the limitations of firewalls?　　　　　　　　　　　　　　　　　　[2]
　j)　What is intruder?　　　　　　　　　　　　　　　　　　　　　　　　　　　[3]

PART-B

(50 Marks)

2.a)　Consider the following:
　　　Plaintext: "KEY"
　　　Secret key: "CRYPTOGRAPHY"
　　　Compute the cipher text from given plain text and key using hill cipher method.
　b)　Explain the model for network security.　　　　　　　　　　　　　　　　[5+5]
OR
3.a)　Explain the transposition techniques.
　b)　What are the advantages of steganography comparing with cryptography?　　[5+5]

4.　　Explain the AES algorithm.　　　　　　　　　　　　　　　　　　　　　[10]
OR
5.a)　Write short notes on key distribution.
　b)　In an RSA system, the public key of a given user is e=31, n=3599. What is the private
　　　key of this user?　　　　　　　　　　　　　　　　　　　　　　　　　　[5+5]

6.　　Explain whirlpool algorithm.　　　　　　　　　　　　　　　　　　　　[10]
OR
7.　　Explain X.509 authentication service.　　　　　　　　　　　　　　　　　[10]

8.   Explain the operation PGP message generation and message reception.   [10]

                                        OR

9.a)   What are the cryptographic algorithms used in S/MIME?
  b)   Draw and explain fields in AH header.   [5+5]

10.   Explain secure inter branch payment transactions.   [10]

                                        OR

11.a)   What is password management?
  b)   What are the various virus counter measures?   [5+5]

                                   ---ooOoo—