Code No: 126AQ **R13**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, October/November - 2016
INFORMATION SECURITY
(Computer Science and Engineering)

Time: 3 hours **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)	Explain the network security model.	[2]
b)	What are the two basic functions used in encryption algorithms?	[3]
c)	What are the advantages of Key Distribution?	[2]
d)	What are the principles of public key cryptosystems?	[3]
e)	List three approaches to Message Authentication.	[2]
f)	Explain the importance of knapsack algorithm.	[3]
g)	What are different approaches to Public-key Management?	[2]
h)	How does PGP provides public key management?	[3]
i)	What is Secure Socket Layer?	[2]
j)	What are different alert codes of TLS protocol?	[3]

PART - B

(50 Marks)

2.a) Explain the terminologies used in Encryption.
b) Describe in detail about Conventional Encryption Model. [5+5]

OR

3.a) Compare symmetric and asymmetric key cryptography.
b) What is Steganography? Explain its features. [5+5]

4.a) Differentiate linear and differential crypto-analysis.
b) Explain Block Cipher design principles. [5+5]

OR

5. Briefly explain the characteristics and operations of RC4 Encryption algorithm. [10]

6.a) What are the requirements of Authentication?
b) Discuss about Secure Hash algorithm. [5+5]

OR

7.a) Explain the approaches for Digital Signatures based on Public Key Encryption.
b) Discuss about Biometric Authentication. [5+5]

8. Briefly discuss about different services provided by Pretty Good Privacy (PGP). [10]

OR

9. What are different cryptographic algorithms used in S/MIME? Explain how S/MIME is better than MIME. [10]

10.a) List and briefly define the parameters that define an SSL session state.
b) What are different services provided by the SSL Record Protocol? [5+5]

OR

11.a) What is a Firewall? Explain its design principles and types with example.
b) Discuss about Password Management. [5+5]

---ooOoo---