Code No: 126AQ

R13

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year II Semester Examinations, May - 2017
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)	Give various security services.	[2]
b)	What are the principles of security?	[3]
c)	Define Stream ciphers?	[2]
d)	Discuss about Blowfish.	[3]
e)	What is Biometric authentication?	[2]
f)	Discuss various Digital signatures.	[3]
g)	Give features of Authentication Header.	[2]
h)	Explain IP Security.	[3]
i)	How to manage the password?	[2]
j)	Discuss cross site scripting vulnerability.	[3]

PART - B

(50 Marks)

2.a) Discuss in detail about various types of Security attacks with neat diagrams.
  b) Give a model for Network Security with neat diagram. [5+5]

OR

3.a) What is symmetric key cryptography? Discuss its advantages and limitations.
  b) Explain various substitution techniques with suitable examples. [5+5]

4.a) Explain DES algorithm with suitable examples. Discuss its advantages and limitations.
  b) What is Elliptic Curve Cryptography (ECC)? Discuss ECC algorithm with neat diagram. [5+5]

OR

5.a) Explain RSA algorithm with suitable examples.
  b) Write a short note on RC4. [5+5]

6.a) Write a short note on knapsack algorithm.
  b) Give various Hash Functions. Discuss secure hash algorithm with suitable examples. [5+5]

OR

7.a) Discuss HMAC and CMAC.
  b) Write a short note on Kerberos. [5+5]

8.a)   Write a short note on Pretty Good Privacy.
  b)   Give IP Security architecture with neat diagram.   [5+5]

OR

9.a)   Write a short note on S/MIME.
  b)   Discuss in detail encapsulating security payload.   [5+5]

10.a) What is Intrusion? Discuss Intrusion detection system with neat diagram.
   b) Discuss the need of Secure Socket Layer.   [5+5]

OR

11.a) Write a short note on firewall design principles and types of firewalls.
   b) Discuss in detail about secure electronic transaction.   [5+5]

---ooOoo---