Mumbai University Question Paper

Network Security

B.Sc.IT: Semester – V

April – 2014

Time: 2 ½ Hours **Total Marks:** 60

N.B.: **(1)** *All Question are Compulsory.*
(2) *Make Suitable Assumptions Wherever Necessary And State The Assumptions Made.*
(3) *Answer To The Same Question Must Be Written Together.*
(4) *Number To The Right Indicates Marks.*
(5) *Draw Neat Labeled Diagrams Wherever Necessary.*
(6) *Use of Non – Programmable Calculator is allowed.*

Q.1 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) What are the Key Principles of Security? Brief them. **(5)**
(B) Explain the different Active Attack? **(5)**
(C) Write Short Notes On: **(5)**
(i) *Mono-Alphabetic Cipher*
(ii) *Rail Fence Technique*
(D) Describe the Diffie-Hellman Key Exchange Algorithm with an example. **(5)**

Q.2 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) What are Algorithmic Modes? Explain the working of Cipher Feedback Mode. **(5)**
(B) How the Key Transformation is done in DES? What is the purpose of XOR and Swap Operations with respect to DES? **(5)**
(C) Compare the processes of RC4 and RC5. **(5)**
(D) Explain the purpose of Subkey Generation in Blowfish. **(5)**

Q.3 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) What is Asymmetric Key Cryptography? How does it work? **(5)**
(B) Describe the RSA Algorithm with an example. **(5)**
(C) State the requirements for a Message Digest by a Sample Digest. **(5)**
(D) What are the problems faced in Public Key Exchange? **(5)**

Q.4 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) Write Short Notes On: **(5)**
(i) *Digital Certificates*
(ii) *Certifying Authority*
(B) Describe the five Architecture Areas of PKIX Model. **(5)**
(C) What are Hash Functions? Explain its working. **(5)**
(D) Explain the Station to Station Protocol. **(5)**

Q.5 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) Explain the TCP Segment Format with a neat diagram. **(5)**
(B) What is an Application Gateway? How does it differ from Packet Filters? **(5)**
(C) Describe the Handshake Protocol of SSL. **(5)**
(D) What are the processes of SET? **(5)**

Q.6 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) State the different steps involved in Clear Text Passwords. **(5)**
(B) Write a Short Notes on Kerberos. **(5)**
(C) What is a Key Distribution Centre? Explain the concept with a diagram. **(5)**
(D) Describe the Mutual Authentication Approach. **(5)**