Mumbai University Question Paper

Network Security

B.Sc.IT: Semester – V

October – 2013

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) Explain the concept of Key Range and Key Size. **(5)**
(B) Define the following terms: **(5)**
- **(i)** *Cryptography*
- **(ii)** *Cryptanalysis*
- **(iii)** *Brute-Force Attack*
- **(iv)** *Symmetric Key Cryptography*
- **(v)** *Asymmetric Key Cryptography*

(C) What are Transposition Techniques? Explain any one with the help of an example. **(5)**
(D) What are the Ethical and Legal Issues in Computer Security System? **(5)**

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

(A) Explain the Cipher Block Chaining Mode of the Algorithm in detail. **(5)**
(B) Explain Blowfish Algorithm and its advantages. **(5)**
(C) Explain the steps in each round of DES. **(5)**
(D) Explain the main features of AES, explain its steps at a high level. **(5)**

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

(A) Explain the basics of Digital Signature. **(5)**
(B) Explain the concept of Message Digest. What are the requirements of the Message Digest? **(5)**
(C) Why HMAC cannot be trusted to be used in Digital Signatures? **(5)**
(D) Explain the security solution based on the concept of Digital Envelope. Explain the security solution based on the concept of Digital Envelope. **(5)**

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

(A) What is Digital Certificate? How is it created? **(5)**
(B) Write a brief note on Cross Certification in Digital Certificates. **(5)**
(C) What are CRLs (Certificate Revocation Lists)? How are they used? **(5)**
(D) Write a brief note on PKCS#5 Password Based Encryption (PBE) Standard. **(5)**

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

(A) Explain the functioning of Packet Filter Firewall. Explain the possible attacks on it. **(5)**
(B) Explain the advantages and applications of IPSec. **(5)**
(C) Explain the concept of Dual Signature in SET (Secure Electronic Transaction). **(5)**
(D) What is PGP? Explain how PGP works. **(5)**

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

(A) Explain Authentication Method based on Challenge/Response Tokens. **(5)**
(B) How does Certificate Based Authentication work? **(5)**
(C) Write a brief note on Kerberos. **(5)**
(D) Explain different approaches of Mutual Authentication. **(5)**