B.Sc.IT: Semester – V
[Network Security]
Question Paper (April – 2017) [75:25 Pattern]

- Kamal T.

Time: 2 ½ Hours **Total Marks: 75**

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.

Q.1	Attempt Any Two of the Question: (10 Marks)	
(A)	Describe the various Security Services.	(5)
(B)	What are Poly-Alphabetic Ciphers? Explaining one technique with suitable example.	(5)
(C)	What is Cryptanalysis? Explain different Cryptanalysis Attacks.	(5)
(D)	What is DDOS Attack? What are the ways in which DDOS attack can be classified?	(5)

Q.2	Attempt Any Two of the Question: (10 Marks)	
(A)	Explain the working of AES Round in detail.	(5)
(B)	Explain the Encryption Operation used in RC5 Algorithm.	(5)
(C)	Explain the working of IDEA Algorithm.	(5)
(D)	Write a note on Blowfish.	(5)

Q.3	Attempt Any Two of the Question: (10 Marks)	
(A)	What is Message Digest? Explain.	(5)
(B)	Explain the working of the SHA Algorithm.	(5)
(C)	What is a Digital Signature? Explain the different categories of verification.	(5)
(D)	Explain the ElGamal Cryptosystems.	(5)

Q.4	Attempt Any Two of the Question: (10 Marks)	
(A)	Explain the Diffie Hellman's Key Agreement Algorithm and its vulnerability.	(5)
(B)	What is Key Pre-Distribution? Explain.	(5)
(C)	Write a note on Station-To-Station Protocol.	(5)
(D)	What is KDC? Explain its different implementations and significance.	(5)

B.Sc.IT: Semester – V
[Network Security]
Question Paper (April – 2017) [75:25 Pattern]

- Kamal T.

Q.5	**Attempt Any Two of the Question: (10 Marks)**	
(A)	What are Firewalls? What are its characteristics and limitations?	**(5)**
(B)	Write a note on IPSec Architecture.	**(5)**
(C)	What is SSL Record Protocol? Explain its operations.	**(5)**
(D)	Explain the Handshake Protocol Action.	**(5)**

Q.6	**Attempt Any Two of the Question: (10 Marks)**	
(A)	Explain the Password Based Authentication System. What are the problems associated with passwords?	**(5)**
(B)	Write a note on Kerberos.	**(5)**
(C)	Explain Biometric Authentication Technique.	**(5)**
(D)	What is Certificate Based Authentication and explain its working.	**(5)**

Q.7	**Attempt Any Three from the Following: (15 Marks)**	
(A)	What are the different goals of Security? Explain the different attacks these Security goals are vulnerable to.	**(5)**
(B)	Explain the working of DES function in details.	**(5)**
(C)	What is Asymmetric Encryption? Explain the RSA Algorithm used for Asymmetric Encryption.	**(5)**
(D)	Explain the concept of Digital Certificate and how it is created?	**(5)**
(E)	What are the approaches used to Detect Intrusion? Give a brief description of each.	**(5)**
(F)	Write a note on Authentication Token.	**(5)**