Ref. No.: Ex/IT/T/424/2017 (Old)

BE IT 4th YEAR 2nd Semester Examination, 2017 (OLD)

NETWORK SECURITY

TIME: 3 Hours

FULL MARKS: 100

Answer Any **FIVE** Questions

1.

a) Describe the different types of attacks to which a cryptographic system may be subjected to. Explain what is meant by the expression "it is infeasible to break a crypto system". 10

b) What are the 5 tuples of cryptosystem? Define a crypto system with these tuples. 5

c) Define and differentiate block cipher and stream cipher in cryptography. 5

2.

a) Describe two main components of stream cipher and what stream cipher encryption algorithm is used in WiFi, GSM and 3G. 4+3

b) Explain secret key cryptography with diagram and example. 3

b) Explain the role of certification in cryptography. 3

c) Explain how a message can be digitally signed using a public key cryptosystem. 7

3.

a) Explain Linear Feedback Shift Register with suitable diagram. 6

b) If the encryption key of a Hill Cipher Cryptosystem is

1	3	3
1	4	3
1	3	4

then, what will be the decryption key? 6

c) Explain the frequency attack and justify whether it is applicable to modern cryptosystem. 4

d) Explain the Key Management advantage of Public Key Cryptosystem over the Symmetric Key Cryptosystem. 4

4.

a) Explain about Monoalphabetic and Polyalphabetic cryptosystems. 4

b) What is a Cryptographic Hash functions. Mention its desirable properties and uses. 5+3

c) Describe Shift Cipher. Why shift cipher is not secure? 6+2

5.

a) Explain a practical implementation of Shannon's S-P network or Feistel Cipher. 8

b) With respect to DES, explain what 'Avalanche Effect' is. 4

c) What are the main building blocks of AES cryptosystem? Describe each of them briefly. 8

6.

a) With respect to Application Layer, Transport Layer and Internet Layer, what are the relevant security protocols which exist in those three layers? 3

b) How application level gateway is different than circuit level gateway? What is Packet filtering router? 4+3

c) What are different mode of operations are available? 4

d) Explain Deterministic encryption and probabilistic encryption? 6

7. Write short note on: 5x4=20

a) Authentication

b) Cipher text only attack

c) Known plain text attack

d) Cryptology

e) Pretty Good Privacy