R09

Code No: 09A60503

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, HYDERABAD

B. Tech III Year II Semester Examinations, June-2014

NETWORK SECURITY

(Common to CSE, IT)

Time: 3 hours **Max. Marks: 75**

Answer any five questions
All questions carry equal marks

- - -

1.a) Explain the model for internetwork security.
b) Write about ARP attacks and man-in-the middle attacks.

2.a) Consider the following:
Plain text : “Cryptography”
Secret Key : “Network”
Find the corresponding cipher text using play fair cipher.
b) Explain Sub-key generation algorithm of Blow fish.

3.a) Consider a Diffie Hellman scheme with a common prime q=11 and a primitive root α=2.
i) If user ‘A’ has public key Y_A=9, what is A’s private key X_A?
ii) If user ‘B’ has public key Y_B=3, what is the shared secret key ‘k’?
b) Explain X.509 strong Authentication procedures.

4.a) Explain the PGP trust model.
b) Write about S/MIME content types.

5.a) What are the various features of Oakley key determination protocol?
b) Draw and explain fields in ESP header.

6.a) Explain the operation of SSL handshake protocol.
b) Explain about Transport Layer Security.

7.a) Explain Digital Immune System.
b) Explain the structure of viruses and various types of viruses.

8.a) What are the attacks can be made on packet filtering routers and their counter measures?
b) Explain about Data Access Control structures.

****