Karunya University
(Karunya Institute of Technology and Sciences)
(Declared as Deemed to be University under Sec.3 of the UGC Act, 1965)

End Semester Examinations - 2015-16 Even Semester - May 2016

14CS2008 Cryptography and Network Security

Set B

Time : 3 hrs
Total Marks: 100

1. a. Draw the general structure of AES and explain each component in detail. (10)

   b. Explain the various transposition techniques with examples.(10)

OR

2. a. Detail the general structure of DES and make clear the encryption decryption process. (15)

   b. Mention the strength and weakness of DES algorithm. (5)

3. a. Give a detailed description of the RSA algorithm with encryption and decryption procedures. (10)

   b. Perform encryption and decryption using RSA algorithm for the following. (10)

   P = 17, q = 31; e = 7; M = 2

OR

4. User A and B use the Diffie-Hellman key exchange technique with a common prime q=11 and a primitive root α =7

   i. If user A has private key Xa=3, what is A's public key Ya? (4)

   ii. If user B has private key Xb=6, what is B's public key? (4)

   iii. . In Diffie-Hellman key exchange detail the procedure involved and prove the existence of secure key transfer. (12)

5. a. With neat diagram explain the Digital Signature Standard algorithm for verifying and signing. (10)

   b. Alice chooses q=11, p=23, h=3 and calculates g. Alice chooses x=7 as the private key and calculates y. Now Alice can send a message to Bob. Assume that H(M)=22 and Alice chooses secret no K=5. Verify the signature. (10)

OR

6. a. Explain SHA-512 and explain one round function with a neat diagram. (10)

   b. Explain the HMAC algorithm with a neat sketch.(10)

7. a. Explain IP security architecture using a neat diagram.(10)

   b. Discuss in detail about Encapsulating security payload. (10)

OR

8. Portray the features of Secure Socket Layer for web security such as SSL Architecture, SSL record protocol, SSL record format and SSL handshake protocol. (20)

9. a. Explain the types of firewalls with real time examples. (10)

   b. Explain the effects of malicious programs towards an effective networking system. (10)

Wishing you All the Best