Code No: **R41051** **R10** **Set No. 1**

IV B.Tech I Semester Supplementary Examinations, October/November - 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

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

Answer any FIVE Questions
All Questions carry equal marks
*****

1. a) What are the elements of symmetric encryption? What are the requirements for secure use of symmetric encryption? [8]
   b) How is ARP attack performed? Explain with an example. [7]

2. a) How do you convert a block cipher into a stream cipher by using the Cipher Feedback (CFB) mode? Explain. [8]
   b) Explain transformation in one round of IDEA. Also explain the key usage in IDEA. [7]

3. a) What is the result of the 5^{15} mod 13 and 456^{17} mod 17 using Fermat's theorem? [8]
   b) Solve the congruence $x^2 \equiv 7$ mod 13, 4444^{4444} mod 18. [7]

4. a) In RSA, Given p=19, q=23 and e=3, find n, $\phi(n)$, and d. [8]
   b) Explain Diffie Hellman Key exchange algorithm. Let p=353 be the prime number and α=3 be its primitive root. Let A and B secret keys of A and B be X_a=97 and X_b=233. Compute the following: (i) Public keys of A and B (ii) Common Secret key. [7]

5. a) Give the structure of HMAC. List out the design objectives of HMAC. Explain the benefits/advantages of HMAC over other hash based schemes. [8]
   b) Explain an attack to which MAC is vulnerable. How to make MAC more secure? [7]

6. a) Explain the authentication procedures defined by X.509 certificate. Illustrate the concept of 'certificate chain' for verification of digital signature on X.509 certificate. [8]
   b) What are the main features of Kerberos Version 5? [7]

7. a) Explain the architecture of IPSec. What are the different headers appended for providing authentication and encryption? [8]
   b) Explain about key management ISAKMP. [7]

8. a) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies? [8]
   b) What bastion host? What are its characteristics? [7]