USN | 1 | S | I | | | | | | | | CS73

Siddaganga Institute of Technology, Tumkur – 572 103

(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belgaum, Approved by AICTE, New Delhi, Accredited by NBA, New Delhi, An ISO9001:2008 Certified)

Seventh Semester B.E. Computer Science & Engg. Examinations May-June 2012

Cryptography & Network Security

Time: 3 Hours **Max. Marks: 100**

Not e : 1. Question No. 1 is Compulsory

2. Answer any 4 full questions from question No. 2 to Question No. 6

1 a) What is message authentication?

b) Using Caesar cipher, encrypt “MEET ME AFTER THE PARTY”.

c) What is steganography?

d) What are the two inputs for any encryption function?

e) State Fermat’s theorem.

f) When is an encryption scheme said to be computationally secure?

g) The primitive operation used in RC4 is ______ .

h) Two integers a and b are said to be congruent modulo n, if ______ .

i) Expand S/MIME.

j) ______ is one of the classes of intruder. 1■10

k) What are the two problems with one-time pad?

ℓ) Describe the role of S-boxes in DES.

m) List the types of cryptanalytic attacks.

n) Give the protocols used to provide IP security.

o) What is the difference between diffusion and confusion? 2■5

2 a) What is meant by single-key encryption? Explain the process of conventional encryption with a neat diagram. 6

b) Differentiate between active and passive attacks, with suitable examples. 6

c) Give the different rules for encrypting two letters at a time using playfair cipher algorithm. Using the same, find the ciphertext for the following message:
M = “Network Security”
Key = “Cryptography”. 8

3 a) Explain DES encryption algorithm with a diagram. Also explain single round of DES encryption algorithm. 12

b) What is meant by meet-in-the-middle attack? Explain triple DES with two keys. 8

4 a) Describe RSA algorithm giving various steps involved in it. 8

b) In a public-key system using RSA, you intercept the ciphertext C=10 sent to a user whose public-key is e=5, n=35. What is the plaintext M? 6

c) Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7.

i) If user A has private key X_A=5, what is A’s public-key Y_A?

ii) If user B has private key X_B=12, what is B’s public-key Y_B?

iii) What is the shared secret key? 6

Please Turn Over

5 a) With proper illustrations, explain any 5 different ways in which a hash code can be used to provide message authentication. 10

b) What is "realm" in kerberos environment? Explain with a suitable diagram, how services between two realms can take place in kerberos. 10

6 a) Explain the IPSec ESP format. Also explain padding and the two ways in which IPSec ESP services can be used. 12

b) Give the taxonomy of malicious programs. Briefly explain each one. 8