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

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 Bachelor of Engineering Examinations Dec.14 – Jan.15

Cryptography and Network Security

Common to Computer Sc. & Information Sc. Engg.

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

Note : 1. Question No. 1 is Compulsory

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

1 a) The service which ensures that only sender and legitimate receivers have access to the content of the message is _______.

b) The service which ensures the recipient that messages is sent by a legitimate uses is _______.

c) When a message is _______, it is an attack on the confidentiality.

d) Define brute force attack.

e) The base key size of DES algorithm is _______.

f) Give equation for Double DES encryption.

g) Given IP function 26314857 IP^{-1}=?

h) The cipher text if "GOD IS GREAT" with Caesar cipher k=7 is _______.

i) A cipher text that encrypts digital data stream one bit or one byte at a time is called _______.

j) A small change in either the plain text or the key should produce significant change in the cipher text. This is called _______.

k) The attack that is based on the linear approximation to describe the transformations in DES is _______.

ℓ) The key length in Double DES is _______.

m) P an q are primes , P>q, n=p■q what is ϕ(n)?

n) What condition makes a and b are relatively prime?

o) In SHA-512, the values in eight 64-bit registers are stored in _______ format.

p) In Public key encryption system, if C=E_{kub} (M), them M=?

q) Name any one functional area of IPsec _______.

r) Define an SSL session.

s) Two modes in which secured IP packets are transmitted are _______.

t) DSS stands for _______. 1■20

2 a) List and explain various services provided in information security. 8

b) Encrypt the following text using Hill cipher technique with the key matrix $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$
text : COMPUTER. 6

c) With a neat block diagram, explain single round of DES encryption. 6

3 a) Show how meet in the middle attack may be applied in double DES method? 5

b) How known plain text attack is applied in triple DES? 5

c) With diagrams, explain OFB encryption and decryption (output feedback). 10

4 a) State and prove Fermat's theorem. List the principles of public key Crypto system. 10

b) Describe RSA algorithm giving various steps involved in it. Given p=17, q=11, e=7, M=88 find a and c. 10

Please Turn Over

5 a) List and explain the differences between Kerberos 4 and 5. 5

b) With a neat diagram explain the key elements of X.509 certificate. 10

c) What is direct digital signature? Explain the scheme along with the possible threats. 5

6 a) Explain how key rings are used in PGP message transmission and reception 10

b) What is a firewall? List its characteristics, explain the function of packet filtering router and its application level gateway (Application proxy). 10