USN | 1 | S | I | 0 | | C | S | | | | CS73

Siddaganga Institute of Technology, Tumkur – 572 103

(An Autonomous Institution under Visvesvaraya Technological University, Belgaum)

Seventh Semester B.E. Computer Science & Engg. Examination May-June 2011

Cryptography and Network Security

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) _____ is a possible danger that might exploit a vulnerability.
b) Represent Masquerade diagrammatically.
c) Define security mechanism.
d) What do you mean by unconditionally secure encryption scheme?
e) Give the ciphertext for 'sit tumkur' using rail fence transposition cipher.
f) List the different names for symmetric encryption.
g) Give one example for stream cipher.
h) What do you mean by a product cipher?
i) Name the two design features of Fiestel cipher.
j) SPN stands for _____
k) List characteristics considered in the design of Blowfish.
ℓ) Define Commutative Ring.
m) List the applications of public-key cryptography.
n) _____is the private key of RSA algorithm.
o) State second version of Fermat's theorem.
p) Write equation for common secret key by user A in Diffie-Hellman key exchange.
q) Define hash function.
r) MAC stands for_____
s) SSL stands for _____
t) List the types of viruses. 1 ▪ 20

2 a) With an example, define authentication security service. 2

b) Differentiate between active and passive attacks. Explain any two types of active attacks. 6

c) In the playfair cipher, the keyword is "BELGAUM". Encrypt the message "CRYPTOGRAPHY IS EASY". 6

d) Demonstrate encryption and decryption using Caesar cipher 6

3 a) With respect to S-DES , generate K1 and K2 for the following data :

Key = 1011001101

P10 = (3 5 2 7 4 10 1 9 8 6)

P8 = (6 3 7 4 8 5 10 9) 4

Please Turn Over

b) With the help of a block diagram explain Fiestel encryption and decryption for 16 rounds. Also show that the output of 1st round of decryption process is equal to a 32-bit swap of the input to the 16th round of the encryption process. 10

c) Explain triple DES with 2 keys. 6

4 a) With an example, define Integral Domain. 2

b) Compute $\Phi(1)$ and $\Phi(7^2)$ using Euler's Totient function. 2

c) Perform encryption and decryption using RSA algorithm .

P = 17 , q = 31 , e = 7 and M = 2 8

d) User A and user B use the Diffie-Hellman key exchange technique, a common prime q = 71 and a primitive root $\alpha = 7$.

i) If user A has private $X_A = 5$, find its public Y_A ?

ii) If user B has private $X_B = 12$, find its public Y_B ?

iii) Determine the shared secret key by both users. 8

5 a) List the different types of authentication functions. Explain briefly, how symmetric message encryption can be used to provide confidentiality and authentication function. 6

b) What is a digital signature? What are its requirements and properties. 8

c) What is Pretty Good Privacy? List the reasons for its growth. 6

6 a) List the applications of IPSec. 4

b) Write a note on web security. 4

c) List and define the three classes of intruders. 4

d) List the three design goals for a firewall. Mention the types of firewalls and briefly explain Packet-filtering router. 8

———————