QP Code: RD17001041 Reg. No | | | | | | | | | | | AR 17

GIET MAIN CAMPUS AUTONOMOUS GUNUPUR – 765022

B. Tech Degree Examinations, December – 2020

(Seventh Semester)

BCSPE 7034 / BITPE 7034 – CYRPTOGRAPHY AND NETWORK SECURITY

(CSE & IT)

Time: 2 hrs Maximum: 50 Marks

The figures in the right hand margin indicate marks.

PART – A: (Multiple Choice Questions) (1 x 10 = 10 Marks)

Q.1. Answer ***ALL*** questions

a. If the sender and receiver use different keys, the system is referred to as conventional cipher system

(i)True (ii)False

b. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.

(i)True (ii)False

c. On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text

(i) nlazeiibljji (ii) nlazeiibljii

(iii) olaaeiibljki (iv) mlaaeiibljki

d. Image obtained after steganography is called _____

(i) Cover image (ii) Stego-image

(iii) Steganalysis (iv) None

e. In asymmetric key cryptography, the private key is kept by _____

(i) sender (ii) receiver

(iii) sender and receiver (iv)all the connected devices to the network

f. Which one of the following algorithms is not used in asymmetric-key cryptography?

(i) RSA algorithm (ii) Diffie-hellman algorithm

(iii) Electronic Code Book algorithm (iv) DSA algorithm

g. What is data encryption standard (DES)?

(i) block cipher (ii) stream cipher

(iii) bit cipher (iv) byte cipher

h. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a

(i)12 (ii)18

(iii)09 (iv)16

i. A computer _____ is a malicious code which self-replicates by copying itself to other

(i) program (ii) virus

(iii) application (iv) worm

j. The Secure Electronic Transaction protocol is used for

(ii) Credit card payment (ii) Cheque payment

(iii) Electronic cash payments (iv) Payments of small amount for internet services

PART – B: (Short Answer Questions) **(2 x 5 = 10 Marks)**

Q.2. Answer ***ALL*** questions

a. List and briefly define Attacks & Its categories of passive and active security attacks.

b. What is the difference between a block cipher and a stream cipher?

c. Explain Double DES and Triple DES structure?

d. Explain Host-Based Intrusion Detection system?

e. Explain briefly about Features of IP Security?

PART – C: (Long Answer Questions) **(6 x 5 = 30 Marks)**

Answer ***ANY FIVE*** questions		Marks
3.	Briefly Explain about Security Services and Mechanisms?	7
4.	Plaintext- INSTRUMENTS, Keyword- MONARCHY, Generate Cipher text using Play fair Cipher Model?	10
5.	Write short notes on Chinese Remainder theorem with examples?	8
6.	Draw the general structure of DES and explain the encryption/ decryption process?	7
7.	Explain RSA Encryption technique with Example?	7
8.	Differentiate MD5 & SHA Hash Algorithm?	8
9.	Explain PGP method in Electronic Mail system?	7
10.	Explain Transport Layer protocol in Web security?	8

--- End of Paper ---