QPC: RN18001230 AR - 18 Reg. No. □□□□□□□□□□

GIET MAIN CAMPUS AUTONOMOUS GUNUPUR – 765022

B. Tech Degree Examinations, November – 2021

(Seventh Semester)

BCSPE7031 / BITPE7031 – CRYPTOGRAPHY AND NETWORK SECURITY

(CSE)

Time: 3 hrs Maximum; 100 Marks

Answer ALL Questions

The figures in the right hand margin indicate marks.

PART – A: (Multiple Choice Questions) (2 x 10 = 20 Marks)

Q.1. Answer ***ALL*** questions [CO#] [PO#]

a. If the sender and receiver use different keys, the system is referred to as conventional cipher system [CO1] [PO1]

(i)True (ii)False

b. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former. [CO1] [PO1]

(i)True (ii)False

c. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text [CO1] [PO1]

(i) nlazeiibljji (ii) nlazeiibljii

(iii) olaaeiibljki (iv) mlaaeiibljki

d. Image obtained after steganography is called _____ [CO1] [PO1]

(i) Cover image (ii) Stego-image

(iii) Steganalysis (iv) None

e. In asymmetric key cryptography, the private key is kept by __________ [CO2] [PO1]

(i) sender (ii) receiver

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

f. Which one of the following algorithm is not used in asymmetric-key cryptography? [CO1] [PO1]

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

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

g. What is data encryption standard (DES)? [CO2] [PO1]

(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 [CO2] [PO1]

(i)12 (ii)18

(iii)09 (iv)16

i. A computer ________ is a malicious code which self-replicates by copying itself to other [CO3] [PO1]

(i) program (ii) virus

(iii) application (iv) worm

j. The Secure Electronic Transaction protocol is used for [CO4] [PO1]

(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 10 = 20 Marks)

	Q.2. Answer ***ALL*** questions	[CO#]	[PO#]
a.	List and briefly define Attacks & Its categories of passive and active security attacks.	[CO1]	[PO2]
b.	List and briefly define categories of security services & security mechanism.	[CO1]	[PO2]
c.	Differentiate Monoalphabetic cipher and Polyalphabetic cipher?	[CO1]	[PO2]
d.	What is the difference between a block cipher and a stream cipher?	[CO2]	[PO2]
e.	Which parameters and design choices determine the actual algorithm of a Feistel cipher?	[CO2]	[PO2]
f.	Explain Double DES and Triple DES structure?	[CO2]	[PO2]
g.	Explain Digital signature?	[CO3]	[PO2]
h.	Define methods of Hash Function?	[CO3]	[PO2]
i.	Explain Host-Based Intrusion Detection system?	[CO3]	[PO2]
j.	Explain briefly about Features of IP Security?	[CO4]	[PO2]

PART – C: (Long Answer Questions) (15 x 4 = 60 Marks)

	Answer ***ALL*** questions	Marks	[CO#]	[PO#]
3. a.	Briefly Explain about Security Services and Mechanisms?	8	[CO1]	[PO3]
b.	Briefly Explain about Symmetric Cipher Model?	7	[CO1]	[PO3]
	(OR)			
c.	Encrypt the following using play fair cipher using the **keyword MONARCHY, Plain Text- "SWARAJ IS MY BIRTH RIGHT".**	8	[CO1]	[PO4]
d.	Explain in detail Transposition Technique With Example?	7	[CO1]	[PO3]
4. a.	Write short notes on Fermat and Euler's theorem?	8	[CO1]	[PO3]
b.	Write short notes on Chinese Remainder theorem with examples?	7	[CO1]	[PO4]
	(OR)			
c.	Draw the general structure of DES and explain the encryption/ decryption process?	8	[CO2]	[PO3]
d.	How AES is used for encryption/decryption?	7	[CO2]	[PO3]
5. a.	Explain RSA Encryption Technique with Example?	8	[CO2]	[PO3]
b.	Differentiate MD5 & SHA Hash Algorithm?	7	[CO2]	[PO3]
	(OR)			
c.	Write short Notes on Firewall?	8	[CO3]	[PO3]
d.	Define Network Based Intrusion Detection System?	7	[CO3]	[PO3]
6. a.	Explain PGP method in Electronic Mail system?	8	[CO4]	[PO3]
b.	Explain briefly Secure Electronic Transaction (SET)?	7	[CO4]	[PO3]
	(OR)			
c.	Differentiate IP4 and IP6 security?	7	[CO4]	[PO3]
d.	Explain use of Transport Layer protocol in Web security?	8	[CO4]	[PO3]

--- End of Paper ---