QPC: RD20BTECH399 AR 20 Reg. No | | | | | | | | | | |

GIET UNIVERSITY, GUNUPUR – 765022

B. Tech (Fifth Semester – Regular) Examinations, December – 2022

BPECS5053 – Information Security

(CSE)

Time: 3 hrs Maximum: 70 Marks

Answer ALL Questions

The figures in the right hand margin indicate marks.

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

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

a. Identify the term which denotes that only authorized users are capable of accessing the information CO-1 PO-2

(i)Confidentiality (ii)Availability

(iii)Integrity (iv)Non-Repudiation

b. State whether True or False: Data encryption is primarily used to ensure confidentiality. CO-1 PO-1

(i)True (ii)False

(iii) Cannot be interpreted (iv) None

c. Passwords enable users to CO-1 PO-2

(i) get into the system quickly (ii) make efficient use of time

(iii) retain confidentiality of files (iv) simplify file structures

d. Which will not harm computer resources CO-2 PO-1

(i)Firewall (ii)virus

(iii)Trojan horse (iv) DoS

e. A Program designed to destroy data on your computer which can travel to "infect" other computers is called a _ CO-2 PO-2

(i) disease (ii) torpedo

(iii) hurricane (iv) virus

f. Verification of a login name and password is known as: CO-2 PO-3

(i) Configuration (ii) Accessibility

(iii) Authentication (iv) Integration

g. __ is a security protocol based on digital certificates. CO-3 PO-3

(i)Digital security (ii) Secure socket layer

(iii) Secure electronic transactions (iv) None of the above

h. _ is an electronic file that uniquely identifies individuals and web sites on the internet and enables secure confidential communications. CO-3 PO-2

(i)Digital certificate (ii)Digital Signature

(iii) SHA (iv) AH

i. Which is mono-alphabatic cipher technique CO-4 PO-2

(i) Vigener cipher (ii) One time pad

(iii) DES (iv)Ceaser cipher

j. Both Public and private key is used in CO-4 PO-1

(i)Symmetric Encryption (ii)Asymmetric Encryption

(iii) Hill cipher (iv) Playfair cipher

PART – B: (Short Answer Questions) **(2 x 10 = 20 Marks)**

Q.2. Answer ***ALL*** questions	[CO#]	[PO#]
a. Define attack in information security.	CO-1	PO-2
b. State security goal in computer.	CO-1	PO-3
c. What do you mean by Integrity in security?	CO-2	PO-2
d. Distinguish between cryptography and steganography.	CO-2	PO-3
e. How brute force attack is used for cryptanalysis?	CO-3	PO-2
f. Apply Vigenere cipher to encrypt GIETU with key CSE.	CO-3	PO-1
g. How many bits of data block used in AES for encryption ?	CO-3	PO-2
h. Write the characteristics of Hash function.	CO-4	PO-4
i. Write the names of protocol used in SSL.	CO-4	PO-1
j. What does the bit fields of alert protocol in SSL explain ?	CO-4	PO-2

PART – C: (Long Answer Questions) **(10 x 4 = 40 Marks)**

Answer ***ALL*** questions	Marks	[CO#]	[PO#]
3. a. List and define security mechanisms used in security standard.	5	CO-1	PO-2
b. What do you mean by cryptography? How is it classified ?	5	CO-1	PO-1
(OR)			
c. Write different security services provided by security protocol.	5	CO-1	PO-1
d. Use play fair cipher to encrypt INTELLIGENT with keyword GIETU	5	CO-1	PO-2
4. a. Compare stream cipher with block cipher techniques	3	CO-2	PO-3
b. Use a Hill cipher to encrypt the message " we live in an insecure world" using the key K= $\begin{matrix} 03 & 02 \\ 05 & 07 \end{matrix}$	7	CO-2	PO-3
(OR)			
c. Explain DES algorithm techniques used for encryption.	10	CO-2	PO-2
5. a. How symmetric encryption is used for remote user authentication?	5	CO-2	PO-2
b. State working of SSL record protocol to provide security services	5	CO-3	PO-1
(OR)			
c. Which protocol does provide security at transport layer? Explain its working	5	CO-3	PO-1
d. Write short notes on Kerberos			
6. a. What is email security? How can it be done ?	5	CO-4	PO-2
b. Define IPSec. Explain its mode of operation	5		
(OR)			
c. Write different steps of SHA-1 algorithms to generate Hash code.	10	CO-4	PO-1

--- End of Paper ---