

--	--	--	--	--	--	--	--	--	--



## GIET UNIVERSITY, GUNUPUR – 765022

### B. Tech (Seventh Semester – Regular) Examinations, November – 2022 BCSPE7034 / BPECT7024 – Cryptography and Network Security (CSE/CST)

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. 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]  
 (iii) Credit card payment (iii) Cheque payment  
 (iv) Electronic cash payments (v) 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 between 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)****(10 x 4 = 40 Marks)**Answer ALL questions

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

--- End of Paper ---