QPC: RN20BTECH669 AR 20 Reg. No

GIET UNIVERSITY, GUNUPUR – 765022

B. Tech (Seventh Semester – Regular) Examinations, November – 2023

BPECS7034 – Cryptography & Network 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. In cryptography, the order of the letters in a message is rearranged by (i) Transpositional ciphers (ii) Substitution ciphers (iii) Both transpositional ciphers and substitution ciphers (iv) Quadratic ciphers	CO1	PO1
b. The inverse of 3 modulo 7 is? (i) -1 (ii) -2 (iii) -3 (iv) -4	CO1	PO1
c. The DES algorithm has a key length of (i) 128 Bits (ii) 32 Bits (iii) 64 Bits (iv) 16 Bits	CO2	PO1
d. When a hash function is used to provide message authentication, the hash function value is referred to as (i) Message Field (ii) Message Digest (iii) Message Score (iv) Message Leap	CO2	PO1
e. What are strengths of Network based IDS? (i) Cost of ownership reduced (ii) Malicious intent detection (iii) Real time detection and response (iv) All of the mentioned	CO3	PO1
f. A computer _____ is a malicious code which self-replicates by copying itself to other programs. (i) program (ii) virus (iii) application (iv) worm	CO3	PO1
g. Which among the following features is present in IPv6 but not in IPv4? (i) Fragmentation (ii) Header checksum (iii) Options (iv) Anycast address	CO4	PO1
h. Unsolicited Bulk E-mails (UBI) are called..... (i) SMS (ii) MMS (iii) Spam emails (iv) Malicious emails	CO4	PO1
i. The linear combination of gcd(10, 11) = 1 can be written as (i) (-1)*10 + 1*11 (ii) (-2)*10 + 2*11 (iii) 1*10 + (-1)*11 (iv) (-1)*10 + 2*11	CO1	PO1
j. Which of them is not a major way of stealing email information? (i) Stealing cookies (ii) Reverse Engineering (iii) Password Phishing (iv) Social Engineering	CO4	PO1

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

Q.2. Answer ***ALL*** questions	[CO#]	[PO#]
a. Differentiate between passive attacks and active attacks.	CO1	PO1
b. Define a threat and an attack.	CO1	PO2
c. Mention the application of public key cryptography.	CO2	PO2
d. Is it possible to use the DES algorithm to generate message authentication code? Justify.	CO2	PO2
e. What is meant by intrusion detection system?	CO3	PO2
f. Define Firewall.	CO3	PO2
g. What do you mean by S/MIME?	CO4	PO2
h. List out the services provided by PGP.	CO4	PO2
i. What do you mean by cryptanalysis?	CO1	PO2
j. State few applications of RC4 algorithm.	CO2	PO2

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

Answer ***ALL*** questions	Marks	[CO#]	[PO#]
3. a. Determine the gcd(24140,16762) using Euclid's algorithm.	5	CO1	PO3
b. Explain any two classical ciphers and also describe their security limitations.	5	CO1	PO2
(OR)			
c. Explain Monoalphabetic Ciphers with example.	5	CO1	PO2
d. Explain briefly about Fermat's and Euler's theorem.	5	CO1	PO3
4. a. Write the applications of cryptographic hash functions.	5	CO2	PO2
b. List out the parameters of AES.	5	CO2	PO2
(OR)			
c. Explain about the Elgamal Digital Signature Scheme.	10	CO2	PO3
5. a. What is Application level Gateway?	5	CO3	PO2
b. Define Network IDS.	5	CO3	PO2
(OR)			
c. What is the different Kerberos Terminology?	10	CO3	PO2
6. a. Discuss about the SET in detail.	5	CO4	PO2
b. Explain ISAKMP header.	5	CO4	PO2
(OR)			
c. Explain Transport Layer Security.	5	CO4	PO2
d. Discuss about the PGP.	5	CO4	PO2

--- End of Paper ---