31N2306

B. Tech. III - Sem. (Main) Exam., May – 2023

Cyber Security

3CY4-06 Introduction to Cyber Security

: 3 Hours **Maximum Marks: 70**

uctions to Candidates:

– A: *Short answer questions (up to 25 words) 10 × 2 marks = 20 marks. All* ***ten*** *questions are compulsory.*

– B: *Analytical/Problem solving questions 5 × 4 marks = 20 marks. Candidates have to answer* ***five*** *questions out of* ***seven****.*

t – C: *Descriptive/Analytical/Problem Solving questions 3 × 10 marks = 30 marks. Candidates have to answer* ***three*** *questions out of* ***five****.*

Schematic diagrams must be shown wherever necessary. Any data you feel missing may suitably be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.

Use of following supporting material is permitted during ***examination****. (Mentioned in form No. 205)*

NIL 2. NIL

PART – A

1 What is RC5 algorithm? [2]

2 How does X.509 authentication service works? [2]

3 How does SSL certificate provides web security? [2]

4 Find GCD of two numbers 1220 and 516 using Euclid's method. [2]

5 How does firewall helps in protecting network of any organization? [2]

Q.6 What are the disadvantages of PGP encryption? [

Q.7 What problems does security risk assessment solve? [:

Q.8 What is the difference between qualitative and quantitative risk assessment? [2

Q.9 Describe any four categories of Cyber Crime. [2

Q.10 Differentiate symmetric and asymmetric encryption schemes with example algorithm of each. [2]

PART – B

Q.1 Explain buffer overflow attack with help of memory (stack) layout of a process. [4]

Q.2 How does PGP and S/MIME schemes provide email security? [4]

Q.3 What do you understand by replay attack and how does Needham Schroeder algorithm ensures safety against replay attack? [4]

Q.4 Explain DOS and DDOS attack architecture. Explain defense techniques to prevent for these attacks. [4]

Q.5 Write short note on - [4]

(a) Spyware

(b) Ransom ware

(c) Adware

(d) Malware

Q.6 Describe classical encryption techniques including substitution and transpose ciphers. [4]

Q.7 Explain legal, ethical and professional issues in information security. [4]

PART – C

Q.1 (a) Explain RSA algorithm in detail.

(b) Let P = 17 and Q = 11 for RSA algorithm then find one possible set of values for E (public key) and D (Private key).

Q.2 What is the importance of Diffie-hellman key exchange? Explain how two parties end up in calculating same value at the end of Diffie-hellman algorithm.

Q.3 How hashing function ensures data integrity? Differentiate MD~~9~~ 5 and SHA~~4~~ -I hash algorithms.

Q.4 Provide detail comparison of AES and DES encryption standards.

Q.5 What is the role of IDS in providing security to any organization? Describe different types of IDS.
