Seat No: _____________ Enrollment No: ___________________

PARUL UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

B.Tech. Winter 2022 - 23 Examination

Semester: 7 **Date: 08/10/2022**
Subject Code: 203105447 **Time: 10:30 am to 01:00 pm**
Subject Name: Network Security **Total Marks: 60**

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Make suitable assumptions wherever necessary.
4. Start new question on new page.

Q.1 Objective Type Questions - (Fill in the blanks (1-5), identify whether statement true or false (6-10), MCQs - (11-15)) **(15)**

(All are compulsory) (Each of one mark)

1. The full form of malware is ____________.
2. _____________ is a code injecting method used for attacking the database of a system / website.
3. When there is an excessive amount of data flow, which the system can not handle, _________ attack takes place.
4. An attempt to harm, damage or cause threat to a system or network is broadly termed as _________.
5. In asymmetric key cryptography, the private key is kept by _________.

6. Network Security provides authentication and access control for resources.
a) True
b) False

7. Data encryption is primarily used to ensure confidentiality.
a) True
b) False

8. Hashes can be used to make sure messages and files transmitted from sender to receiver are not tampered with during transit.
a) True
b) False

9. The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's public key.

a) True
b) False

10. Trojan horses are very similar to virus in the matter that they are computer programs that replicate copies of themselves
a) True
b) False

11. Failed sessions allow brute-force attacks on access credentials. This type of attacks are done in which layer of the OSI model?
a) Physical layer
b) Data-link Layer
c) Session layer
d) Presentation layer

12. Security features that control access resources in the OS.
a) Authentication
b) Identification
c) Validation
d) Access control

13. Which of the following is not an application of Euclid's algorithm?
a) Simplification of fractions
b) Performing divisions in modular arithmetic
c) Solving quadratic equations
d) Solving Diophantine equations

14. What is data encryption standard (DES)?
a) block cipher
b) stream cipher
c) bit cipher
d) byte cipher

15. A cryptographic hash function is an equation used to verify the ______ of data.
a) Variety
b) Validity
c) Veracity
d) None of the mentioned above

Q.2 Answer the following questions. (Attempt any three) **(15)**
A) What are the different types of security attacks?
B) How the Euclidean Algorithm is useful?
C) What are the Block Cipher Design Principles?
D) How digital signature enhances security?

Q.3 A) Explain in detail the OSI security architecture? **(07)**
B) Differentiate between cyber diseases versus biological diseases? **(08)**

OR

B) With the help of example explain the RSA Algorithm in detail? **(08)**

Q.4 A) Explain in detail Fermat's and Euler's Theorems? **(07)**

OR

A) Explain in detail Symmetric Key Distribution Using Asymmetric Encryption? **(07)**
B) How Symmetric Cipher Model is useful in various ways? **(08)**