Name:

Enrolment No:

UPES

End Semester Examination, May 2023

Course: Information Security **Semester: IV**
Program: BSc Geology **Time : 03 hrs.**
Course Code: MATH2022G **Max. Marks: 100**

Instructions: All questions are compulsory. Internal choice available in Q 9 and Q 11.

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	What is Avalanche Effect in Cryptography?	**4**	**CO4**
Q 2	Differentiate between Authentication and Authorization.	**4**	**CO1**
Q 3	Write down the benefits of Auditing and Logging?	**4**	**CO3**
Q 4	What is Man-in-the-middle (MITM) attack?	**4**	**CO2**
Q 5	Write short notes on the following: a) Phishing b) Identity Theft	**4**	**CO5**

SECTION B
(4Qx10M= 40 Marks)

Q 6	Describe all the elements of information security with examples.	**10**	**CO1**
Q 7	What is Digital Signature? Explain with an example. Differentiate between Hash, MAC, and Digital Signature.	**10**	**CO5**
Q 8	Define the following term with example: a) Risk [3] b) Threat [3] c) Vulnerability [2] d) Exploit [2]	**10**	**CO4**
Q 9	Discuss the classification of intrusion detection systems and intrusion prevention systems. OR Compare and contrast intrusion detection system and intrusion prevention system.	**10**	**CO3**

SECTION-C
(2Qx20M=40 Marks)

Q 10	Differentiate between the following: a) Trojan v/s Worm [05] b) Symmetric v/s Asymmetric encryption [05] c) Monoalphabetic v/s Polyalphabetic Ciphers [05] d) Steganography v/s Cryptography [05]	**20**	**CO2**
Q 11	a) Write and explain the RSA algorithm. [10] b) In a public key cryptosystem using RSA algorithm, a user uses two prime numbers 5 and 7. He chooses 11 as encryption key, find out decryption key. What will be the cipher text if the plaintext is 2? [5+5] OR Discuss about DES algorithm and draw the complete architecture. [20]	**20**	**CO6**