Name:

Enrolment No:

UPES

UNIVERSITY OF TOMORROW

UPES

End Semester Examination, December 2023

Course: Cryptography and Network **Semester : V**

Program: B Sc (H) Geo **Time : 03 hrs.**

Course Code: MATH2021G **Max. Marks: 100**

Instructions: Attempt all questions.

SECTION A

(5Qx4M=20Marks)

S. No.		**Marks**	**CO**
Q1	i. Explain Kirchhoff's Principle in cryptology. ii. Point out the differences between PRF and PRP.	**1+3**	**CO1**
Q2	i. Explain a PRG. ii. Explain encryption using PRGs.	**2+2**	**CO1**
Q3	Write a short note on TCP Session Hijacking.	**4**	**CO2**
Q4	Write a short note on Tunneling using IPSEC.	**4**	**CO3**
Q5	Describe Firewall characteristics & design principles.	**4**	**CO5**
SECTION B **(4Qx10M= 40 Marks)**			
Q6	Describe Denial of Service (DOS) Attacks: i. SYN Flood ii. Teardrop attacks iii. Land iv. Smurf Attacks	**2.5*4**	**CO2**
Q7	Describe the IP security Architecture	**10**	**CO3**
Q8	Describe SNMP Architecture.	**10**	**CO4**
Q9	Write Firewall Characteristics & Design Principles.	**10**	**CO5**
SECTION-C **(2Qx20M=40 Marks)**			
Q10	i. Describe are the different types of Firewalls? ii. Describe Secure Socket Layer and Secure Electronic Transaction	**10+10**	**CO5**
Q11	i. Describe DH-Key Exchange protocol. ii. Describe man-in-the-middle attack in DH-Key Exchange protocol.		

	iii. Describe RSA-Cryptosystem with an example. iv. Identify the mathematical hardness assumption behind security of RSA and DH? OR i. Explain the various adversarial goals in Cryptography. ii. Explain “Shannon Cipher is unusable in practical applications.” iii. Describe meet-in-the-middle attack in DES. iv. Describe how it is solved using 3DES. v. With clear diagram describe any 4 mode of operations of a blockcipher.	**5+5+8+2 OR 2.5*4+10**	**CO1**