UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2021

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

Instructions:

	SECTION A **(Scan and upload) (5Qx 4M = 20 Marks)**		
Q 1	Create a cipher for key=3 and Text=”EXAM” using Substitution Cipher.	**4**	**CO1**
Q 2	Create a cipher for key=2134 and Text=”UPES” using Transposition Cipher	**4**	**CO2**
Q 3	Explain Trojan Horse with relevant example.	**4**	**CO3**
Q 4	Differentiate between worms and virus.	**4**	**CO4**
Q 5	Explain the steps to find primitive root of any prime number X in the presence of galosis field value Y.	**4**	**CO5**
	SECTION B **(Scan and upload) (4Qx10M = 40 Marks)**		
Q 1	Explain playfair cipher with encryption and decryption rules in detail.	**10**	**CO4**
Q 2	Draw a block diagram to portray hash function on plaintext.	**10**	**CO2**
Q 3	Differentiate between symmetric and asymmetric cipher	**10**	**CO1**
Q 4	Write a short note on auditing and logging.	**10**	**CO3**
	OR		
Q 4	What are the steps to detect an intrusion?	**10**	**CO3**
	SECTION-C **(Scan and upload) (2Qx 20M= 40 Marks)**		
Q 1	Draw a block diagram for simplified version of Data encryption standard (DES) for 2 rounds. Assume key K1 and K2.Represent for 2 x 2 dimension of substitution box.	**20**	**CO 3**
Q 2	Explain RSA algorithm in detail with proper case study	**20**	**CO 4**
	OR		
Q 2	Explain an execution of Extended Euclid algorithm with numerical steps for prime number 33 in GF value 1067.	**20**	**CO 4**