Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, July 2020

Course: **Network Security and Cryptography** **Semester: VIII**
Program: **B.Tech(EE+BCT)** **Time 03 hrs.**
Course Code: ELEG355 **Max. Marks: 100**

Instructions: Answer the following questions

SECTION A

S. No.		Marks	CO
Q1	What is the difference between a Stream Cipher and a Block Cipher?	**5**	**CO1**
Q2	Write any one technique of attacking RSA	**5**	**CO3**
Q3	What is meant by the Diffie-Hellman key exchange?	**5**	**CO4**
Q4	Explain about classical crypto systems (substitution and transposition)with two examples for each.	**5**	**CO2**
Q5	Explain in properties of Hash Functions.	**5**	**CO4**
Q6	Find GCD of 1070and 1066 using Euclid algorithm.	**5**	**CO1**
	SECTION B		
Q7	What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end differentiate digital signature from digital	**10**	**CO4**
Q8	Briefly describe the idea behind Elliptic Curve Cryptosystem and describe the key management of public key	**10**	**CO2**
Q9	Encrypt the message "PAY" using hill cipher with the following key matrix and show the decryption to formulate original plaintext K= {17 ,17, 5; 21, 18, 21; 2, 2, 19}	**10**	**CO5**
Q10	Explain the DES key generation algorithm	**10**	**CO3**
Q11	Summarize the Operations of PGP ? Brief the various services provided by PGP **OR** List the different types of attacks and explain in detail. **(10 Marks)**	**10**	**CO1, CO4**
	SECTION-C		
Q12	A). Summarize the Operations of PGP ? Brief the various services provided by PGP. **(10 Marks)** OR Analyze the Cryptographic algorithms used in S/MIME and Explain S/MIME certification processing **(10 Marks)** B). Where hash functions are used? What characteristics are needed in secure hash Function? Write about the security of hash functions and MACs **(10 Marks)** OR Analyze the MD5 message digest algorithm with necessary block **(10 Marks)**	**20**	**CO4, CO2**