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

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

Course: **Network Security and Cryptography** **Semester: VIII**
Program: **B.Tech(EE+BBCT)** **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	Explain the extended Euclid's algorithm with example	**5**	**CO3**
Q3	Briefly explain Deffie Hellman key exchange with an example.	**5**	**CO4**
Q4	Compare the Features of SHA-1 and MD5 algorithm.	**5**	**CO2**
Q5	Explain in properties of Hash Functions.	**5**	**CO4**
Q6	Explain about classical crypto systems (substitution and transposition)with one examples for each.	**5**	**CO1**
	SECTION B		
Q7	Encrypt and decrypt the message M="CS" using RSA algorithm for the following parameters; p=7; q=11; e=17;	**10**	**CO4**
Q8	What are the different modes of operation in DES?	**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	Explain the extended Euclid's algorithm to find all the multiplicative inverse of Z_8 and Z_{11} **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 Apply Caesar cipher and k=5 decrypt the given Ciphertext "YMJTYMJWXNIJTKXNQJSHJ" **(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	**20**	**CO4, CO2**

	Discuss the following i) Message Integrity ii) Denial of Service iii) Availability iv) Authentication**(10 Marks)**		