Roll No: --------------------------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, April 2018

Program: Btech O&G, OSS, CCVT, BAO, TI and CSERA **Semester – VIII**

Subject (Course): Cryptography and Network Security **Max. Marks : 100**
Course Code : CSEG 423 **Duration : 3 Hrs**
No. of page/s:02

SECTION A

All questions are Compulsory **[Marks 6*10=60]**

1. Explain Pretty good privacy .
2. Encrypt the text “College Over” and key UPES by using play fair cipher.
3. Explain the method to find primitive roots and relatively prime numbers.
4. Explain S –box architecture of 64 bit DES.
5. Write a short note on various versions of SHA algorithm.
6. What do you mean by digital signature? Compare digital signature with traditional signature system from the perspective of security.

SECTION B

Attempt any two questions **[Marks 2*20=40]**

Que 1:

A. Explain fiestal cipher with proper block diagram . [Marks 10]

B. Explain the handshake protocol of SSL? [Marks 10]

Que 2:

A. Explain DSS algorithm for digital signature along with proper diagram. [Marks 10]

B Differentiate between substitution and transposition technique. [Marks 10]

Que 3:

A Draw diagrammatic representation and communication structure of Kerberos 4.0 and Kerberos 5.0 ,Discuss advantages and limitations.

[Marks 20]