UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, April/May 2018

Program: B. Tech CS+CL **Semester – VI**
Subject (Course): Network Security and Cryptography **Max. Marks : 100**
Course Code : CSEG 423 **Duration : 3 Hrs**
No. of page/s: 2

Instructions:
Section-A: Answer all the questions and each question carries equal marks (4x5=20 Marks**)**
Section-B: Answer all the questions each question carries equal marks (4x10=40 Marks**)**

Section-C: Answer any two questions each question carries equal marks (2x20=40)

SECTION A

S. No.		**Marks**	**CO**
Q 1	Which attacks threatens Integrity?	**5**	**CO1**
Q 2	List few Password Selection Strategies?	**5**	**CO1**
Q 3	How Synchronous Modern Stream Ciphers operate?	**5**	**CO3**
Q 4	What is Clogging attack in IPSec.	**5**	**CO4**

SECTION B

Q5	Discuss various categories of Traditional Ciphers with two elaborative examples for each.	**10**	**CO4**
Q6	Can you explain difference between X.509 and PGP Certificates? Provide details.	**10**	**CO4**
Q7	How Digital Signature and Message Authentication Code work?	**10**	**CO3**
Q8	Advanced Encryption Standard (AES) is a Block Cipher. Draw structure of AES and explain Key Expansion operation. OR Passwords are poised with certain vulnerabilities. List them all. Elaborate few protection mechanisms for password.	**10**	**CO2**

SECTION-C

Q 9	(a) Is Security Association is really important? Explain related aspects like SAD and SPD. (10) (b) What you understand by Message Authentication Codes (MAC)? Explain SHA	**20**	**CO4 and CO5**

	512 structure and operations. OR (a) Explain how Kerberos operates. (b) What are tunnel and transport modes in IPSec? What is the usage of IKE in IPSec?		
Q 10	Why we require Secure Session Layer (SSL)? Which components are used in SSL? Discuss each with internal details of each component.	**20**	**CO4**