Name: **Enrolment No:**	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2022

Course: Information Security Fundamentals **Semester: V**
Program: B.Tech-CSE-Minor **Time : 03 hrs.**
Course Code: CSSF 2001P **Max. Marks: 100**

Instructions: Attempt all questions.

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	Justify the need for *CIA Triad* with appropriate examples. "An employee not having the appropriate authorization should not be allowed to view the payroll details or the personal information of other colleague" –This example related to which of the CIA Triad property?	**3+1**	**CO1**
Q 2	"The mixer in the Feistel Cipher design is self-invertible"-Justify.	**4**	**CO3**
Q 3	Identify the need for firewall. Discuss different types of firewall.	**2+2**	**CO2**
Q 4	Distinguish between digital signature and digital certificates.	**4**	**CO3**
Q 5	Find the number of padding bits in SHA -512 if the length of the original message is 2590 bits?	**4**	**CO3**
	SECTION B **(4Qx10M= 40 Marks)**		
Q 6	Define protection against malware? Discuss various solutions for protection against malware.	**3+7**	**CO1**
Q 7	Describe various types of attacks generally found in network security.	**10**	**CO4**
Q 8	Analyze the need for operating system security. Discuss different types of operating systems in detail.	**4+6**	**CO2**
Q 9	Distinguish between DES and AES cryptographic algorithm.	**10**	**CO3**
	SECTION-C **(2Qx20M=40 Marks)**		
Q 10	(a) Distinguish between symmetric key and asymmetric key cryptography. (b) Jennifer creates a pair of keys for herself. She chooses p = 397 and q = 401. She calculates n = 397 × 401= 159197. She then calculates φ (n) = 396 × 400 = 158400. She then chooses e = 343 and d = 12007. Suppose Ted wants to	**10+10**	**CO3**

	send the message "NO" to Jennifer. Show how Ted can send the message to Jennifer if he knows e and n.		
Q 11	(a) Is hashing safe for passwords? (b) Can hashed passwords be decrypted? (c) How do I know if a password is hashed? (d) Can two passwords have same hash? (e) Do we need padding if the length of the original message is already a multiple of 1024 bits in SHA-512?	**3+3+3 +3+8**	**CO2**