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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2021

Course: Internet Security and Protocols — **Semester: VIII**
Program: B. Tech (CSE + IoT + SC) — **Time: 03 hours**
Course Code: CSSF 4010P — **Max. Marks: 100**

Instructions:

- **Section A** has 6 Questions of 5 marks each, type your answer in the test box.
- **Section B** has 5 Questions for total of 10 marks each, write brief notes with diagrams.
- **Section C** has choice of 2 Questions for total of 20 marks, mention answers with diagrams.
- Use white A4 with black gel-pen; write clearly with diagrams to illustrate your answers.
- Ensure shadows do not fall on the answer paper while clicking/scanning the sheet.
- Double check quality of the scanned/photograph of the answer before uploading.
- If answer is more than one page long, mention section & answer number on each page.

SECTION A

S. No.		Marks	CO
Q 1.	You and Karan are exchanging emails securely. When sending your emails, you use a key to encrypt them. However, you are unable to decrypt the emails received when using the same key that was used to encrypt them. What best describes this scenario? a.) Email clients don't support cryptography b.) Asymmetric cryptography is being used c.) Stream Cipher is being used d.) Block Cipher is being used.	**5**	**CO1**
Q 2.	Which of these statements is incorrect? a.) Symmetric key algorithms use the same private key to encrypt and decrypt b.) Symmetric key algorithms are often referred to as public key algorithms c.) ECC is an example of an asymmetric public key cryptosystem d.) Symmetric key algorithms are typically faster than asymmetric systems	**5**	**CO1**
Q 3.	Developers often ensure that input to a search function they developed would result in commas, quotes, and other certain special characters being stripped out. Which of the following is likely their reasoning? a.) They are paranoid, and they should allow the original input term to process as is b.) They want to prevent SQL injection by validating the input c.) They want to prevent privilege escalation by providing proper exception handling d.) They are lazy and didn't want to have to refactor their search algorithm	**5**	**CO1**

Q 4.	Your company plans to a new branch office. As IT Security Admin, you are required to provide seamless access from that new branch office to corporate network resources as if they were at the corporate offices. Which of the following would best enable you to accomplish this goal? a.) Machine-to-Machine VPN b.) Site-to-site VPN c.) Spanning Tree Protocol d.) Screened subnet firewall	**5**	**CO2**
Q 5.	UPES IT corporate policy requires use of passphrases instead of passwords. Which of the following technical controls should in place to best promote the use of passphrases? a.) Lockout b.) Length c.) History d.) Complexity	**5**	**CO2**
Q 6.	UPES has web servers in DMZ, these are remotely accessed by the IT Admins remotely from the internal network (campus) over SSH. However, these servers have come under attack via SSH from the IP address 93.184.216.34. Which of the following should you do to stop this attack? a.) Configure a rule to block outbound SSH requests to 93.184.216.34 b.) Shut down the SSH service on all web servers c.) Add rule to block inbound requests on port 22 d.) Add rule to block port 21 inbound requests from 93.184.216.34	**5**	**CO2**
	SECTION B		
Q 1.	a. Explain how public key cryptography can be used for identification. b. What is the purpose of Dual Signatures when linking two messages?	**10**	**CO2**
Q 2.	Describe the Digital Signature Model process with diagrams.	**10**	**CO1**
Q 3.	a. With the explosive growing reliance on emails, there grows a demand for secure communication. Which scheme or approach would you propose and what are the reason for the growth of such authentication and confidentiality services? b. Describe the Services, functions and algorithms associated with PGP.	**10**	**CO3**
Q 4.	a. What does IPSEC provide and describe the architecture? Illustrate your answer with diagrams as required. b. What are the types of IPSEC modes?	**10**	**CO3**
Q 5.	a. What do you understand by SSL Certificate? How does it create secure sessions? b. What do you understand by Keyless SSL?	**10**	**CO3**

SECTION-C			
Q 1.	a. Describe the different types used by Firewalls to block, deny or allow traffic. b. Differentiate NAT and PAT with examples and diagrams. **OR** a. Describe various types of Access Control Lists with examples. b. Describe Content and URL filtering with diagrams.	**20**	**CO4**