Name:

Enrolment No:

UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2019

Course: Security in Cloud — **Semester: VIII**
Program: B.Tech CS+CCVT — **Time 03 hrs.**
Course Code: CSIB471 — **Max. Marks: 100**

Instructions: Read the questions carefully and attempt accordingly

SECTION A

S. No.		Marks	CO
Q 1	Choose the correct (or the most suitable) option: i. The other day while opening the email, you got an interesting but suspicious message from an organization. The message said that “you’ve won the lottery” and the company was asking you specific personal and banking details so that they could lodge a large sum of money in your bank account. These emails are a common type of cyber-attack that goes by the name of: A. Phishing B. Spyware C. Spoofing ii. Patching the operating system: A. Fixes problems and makes the operating system more secure B. Improves the working function of the Operating System iii. What is your perspective about the need for updating the antivirus? A. I have never been a victim of malware. These updates are not relevant to me. B. The antivirus update protects my computer from newly created malware. C. The antivirus updates ensure the correct performance of my computer. iv. On your personal laptop you have been using some of the same computer programs for years. One of your friends, who is an expert in security, noticed that one of your programs has long been discontinued by the manufacturer. Your friend told you that this old	**[4]**	**CO1**

	and discontinued software exposes your computer to serious security threats due to integrity problems. Among these threats your friend mentioned….. A. The Dark Net B. Malicious Software C. Privacy Invasions		
Q2	Choose the correct (or the most suitable) option: i. Whenever you see an interesting app you want it and your instinct is just to download and install it. However, for ensuring your safety and security it is best to… A. Make sure you do not incur hidden costs when downloading an app. B. Check that the app comes from a reputable source. C. Not have too many apps installed, as the use of the smartphone will become difficult. ii. An intruder might install this on a networked computer to collect user ids and passwords from other machines on the network. A. Rootkit B. Token C. Passphrase iii. This type of intrusion relies on the intruder's ability to trick people into breaking normal security procedures. A. Shoulder surfing B. Social engineering C. Hijacking iv. This is a program in which harmful code is contained inside apparently harmless programming or data. A. Snort B. Honey pot C. Trojan horse	**[4]**	**CO4**
Q3	Define Information Security. What are the three pillars of information security?	**[4]**	**CO1**
Q4	In PGP, Find the probability that a user with public keys will have at least one duplicate key ID?	**[4]**	**CO3**
Q5	Find out how many one-to-one affine Caesar ciphers are there for 26 alphabets?	**[4]**	**CO3**
SECTION B			
Q6	Enlist three examples for the following with respect to IAM:	**[10]**	**CO2**

	i. Authentication ii. Authorization iii. User Management iv. Central User Repository		
Q7	Discuss RSA algorithm with example.	**[10]**	**CO3**
Q8	Discuss the core components of AAA? Define each component in short.	**[10]**	**CO1**
Q9	Enlist and Explain the Four SSL Protocol. **OR** Differentiate between SSL Connection and SSL Session.	**[10]**	**CO4**
SECTION-C			
Q10	A). Create a sample checklist for cloud security assessment (at least 10 questions). **[5]** B). Identify the framework which is most suitable for the statement “Providing the right people with the right access at the right time”. Explain in brief the evolution of the framework identified **[10]** C). Enlist with diagram 6 phases of IAM Lifecycle. **[5]**	**[20]**	**CO1, CO2**
Q11	Consider a = 0, b = 1 ……. z = 25. Encrypt the phrase “defend the east wall of the castle” using affine cipher using the key (5, 7). Also show the decryption. **OR** Elaborate the significance of modulus in RSA and also in the RSA public-key encryption scheme, each user has a public key, e, and a private key, d. Suppose Bob leaks his private key. Rather than generating a new modulus, he decides to generate a new public and a new private key. Is this safe? justify your answer with valid argument.	**[20]**	**CO3**

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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2019

Course: Security in Cloud **Semester: VIII**
Program: B.Tech CS + CSF **Time 03 hrs.**
Course Code: CSIB471 **Max. Marks: 100**

Instructions: Read the questions carefully and attempt accordingly

SECTION A

S. No.		Marks	CO
Q 1	How many one-to-one affine Caesar ciphers are there for 26 alphabets?	**[4]**	**CO3**
Q2	Choose the correct (or the most suitable) option: I)This is an encryption/decryption key known only to the party or parties that exchange secret messages. A. Private key B. Public key C. Digital Signature II) In password protection, this is a random string of data used to modify a password hash. A. Dongle B. Salt C. Bypass III) This is a trial and error method used to decode encrypted data through exhaustive effort rather than employing intellectual strategies. A. Cryptanalysis B. Serendipity C. Brute Force IV) What is SSL used for? A. Encrypt data as it travels over a network B. Encrypt files located on a Web server C. Encrypt digital certificates used to authenticate a Web site	**[4]**	**CO3, CO4**
Q3	1. Match the following: **Column A** **Column B**	**[4]**	**CO1**

	1. Natural Threat A. Chemical Damage 2. Environmental Threat B. Power Failure 3. Human Threat – Intentional C. Flood 4. Human Threat – Deliberate D. Data entry error 5. Natural Threat E. Virus Infection 6. Environmental Threat F. Earthquake		
Q4	What do you understand by defense in depth as strategy?	**[4]**	**CO1**
Q5	Identify and explain all types of security goals keeping quality of security in mind.	**[4]**	**CO1**
SECTION B			
Q6	Suggest your understanding by the term 'risk'? What are the four methods of risk management? Explain each with the help of example. **OR** Define and Explain Incident Response Life Cycle with an example.	**[10]**	**CO1**
Q7	Analyze and explain in detail the format for X.509 Certificate.	**[10]**	**CO4**
Q8	Find the working of PGP and elaborate the same with the help of an example.	**[10]**	**CO3**
Q9	Differentiate between chosen cipher text and chosen plain text attack.	**[10]**	**CO3**
SECTION-C			
Q10	Explain the life cycle for Identity and Access Management	**[20]**	**CO2**
Q11	Discuss Caesar's cipher with the help of example. **OR** In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then what will be the private key of A.	**[20]**	**CO3**