UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2020

Course: Information Safety **Semester:** VI
Program: Bachelor of Computer Applications **Time:** 03 hrs.
Course Code: CSBC3003 **Max. Marks:** 100

Instructions: Use of calculators and other electronic devices is prohibited

SECTION A

S. No.		Marks	CO
Q 1	In CIA triad 'A' stands for _____. a)Authenticity b)Availability c)Awareness d)Access	**2**	**CO2**
Q 2	_____ is the practice and precautions taken to protect valuable information from unauthorized access, recording, disclosure or destruction. a) Network Security b) Database Security c) Information Security d) Web Security	**2**	**CO1**
Q 3	Trojan is an example of _____threats. a)Malware b) Network c)Antivirus d)External	**2**	**CO2**
Q 4	Broken Authentication is an example of _____ based threats. a)Network b)Database c)Malware d)Web Application	**2**	**CO3**
Q 5	RSA Algorithm uses _____keys. a)Shift key b)Matrix key c)Asymmetric key d)Symmetric key	**2**	**CO4**
Q 6	PCI stands for _____. a)Paid Credit Information b)Payment Card Information c)Payment Card Industry d) Paid Credit Industry	**2**	**CO4**
Q 7	Which of the following do not comes under Social Engineering? a) Tailgating b) Phishing c) Pretexting d) Spamming	**2**	**CO1**
Q 8	Compromising confidential information comes under _____ a)Bug b)Threat c) Attack d) Vulnerability	**2**	**CO1**
Q 9	Ceaser Cipher uses _____ keys. a)Shift b)Monarchy c)Public d)Private	**2**	**CO3**
Q 10	In which year India's IT Act came into existence? a) 2000 b) 2001 c)2008 d)2010	**2**	**CO4**
Q 11	This is the model designed for guiding the policies of Information security within a company, firm or organization. What is "this" referred to here? a) Confidentiality b) Non-repudiation c) CIA Triad d) Authenticity	**2**	**CO1**

Q 12	In a phishing, attackers target the _____ technology to so social engineering. a) Emails b) WI-FI network c) Operating systems d) Surveillance camera	2	CO2
Q 13	Data _____ is used to ensure confidentiality. a)Encryption b)Locking c)Deleting d)Backup	2	CO2
Q 14	_____ is a weakness that can be exploited by attackers. a) System with Virus b) System without firewall c) System with vulnerabilities d) System with a strong password	2	CO2
Q 15	Cyber-crime can be categorized into _____ types. a)4 b) 2 c) 3 d) 1	2	CO4
Q 16	Stealing pen drives and DVDs after tailgating is an example of lack of _____ security. a) Network security b) Physical security c) Database security d) Wireless security	2	CO2
Q 17	Playfair Cipher is also known as _____. a)Shift Cipher b)Bigraph Cipher c)Diagraph Cipher d)Hill Cipher	2	CO3
Q 18	Decrypt 'FX' using Ceaser cipher taking key as='6' (Take A=1, B=2,..)". a)KD b) OP c) EX d) AS	2	CO3
Q 19	What is the updated version of the IT Act, 2000? a) IT Act, 2007 b) Advanced IT Act, 2007 c) IT Act, 2008 d) Advanced IT Act, 2008	2	CO4
Q 20	For n=323, e=2, message '89' is encrypted as_____ using RSA algorithm. a)24 b)149 c)160 d)169	2	CO3
Q 21	Which of the following is not an example of a computer as weapon cyber-crime? a) Credit card fraudulent b) Spying someone using keylogger c) IPR Violation d) Pornography	2	CO4
Q 22	For d= 3, n=27, message='10' is decrypted as_____ using RSA. a)999 b)1 c)2 d)37	2	CO3
Q 23	A _____ is a software bug that attackers can take advantage to gain unauthorized access in a system. a) System error b) Bugged system c) Security bug d) System virus	2	CO2
Q 24	DoS stands for_____. a)Denial of Services b)Do no Services c)Deny of Services d)Do official Services	2	CO2
Q 25	_____ company suffered one of the largest data breach problem. a)IBM B)Google c)Bing d)Yahoo	2	CO1

Q 26	_____is the technology to hide information inside a picture. a)Visual Cryptography b) Steganography c)Cryptography d)Stenography	2	CO2
Q 27	Which of the following is not a type of cyber crime? a)Data Theft b)Forgery c)Damage to data and systems d)Installing antivirus	2	CO4
Q 28	ISMS is abbreviated as _____ a) Information Server Management System b) Information Security Management Software c) Internet Server Management System d) Information Security Management System	2	CO1
Q 29	What is the name of the IT law that India is having in the Indian legislature? a) India's Technology (IT) Act, 2000 b) Digital Information Technology (DIT) Act, 2000 c) India's Information Technology (IT) Act, 2000 d) The Technology Act, 2008	2	CO4
Q 30	Which of them is not an example of physical hacking? a) Walk-in using piggybacking b) Sneak-in c) Break-in and steal d)Phishing	2	CO3
Section B			
Q 1	Explain the need of information safety with an example.	10	CO1
Q 2	Distinguish between Asymmetric and Symmetric keys. Give examples of each in which algorithms they are used.	10	CO2
Q 3	What are the salient features of IT ACT 2000? OR Discuss the key points of ISO 27001.	10	CO4

| Q 4 | Apply Playfair Cipher algorithm to encrypt the plain text "COME TO THE WINDOW" using the key as "KEYWORD". Also use the same key to decrypt the encrypted text " YIEAESVKEZ"

 OR

 For the given data compute the following using RSA Algorithm:

 a) Public key (n,e)= (33,3) and d=2
    i)   Encrypt the message M=13
    ii)   Decrypt the message M1 =29

 b) p=11, n=143 calculate:
    i)   q
    ii)   phi(n) | 10 | CO3 |