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

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

Course: Internet Security and Protocols — **Semester: VIII**
Program: B.Tech CSE with spz in IoT & Smart Cities — **Time 03 hrs.**
Course Code: CSEG 410 — **Max. Marks: 100**

Instructions: Use headings, quotation, and paragraphs to support your explanations if possible.

SECTION A

S. No.		Marks
Q 1	1. In cryptography, the order of the letters in a message is rearranged by _____ a) transpositional ciphers b) substitution ciphers c) both transpositional ciphers and substitution ciphers d) quadratic ciphers	**CO1** **1*6**
	2.Polyalphabetic ciphers are stronger than Monoalphabetic ciphers because frequency analysis is tougher on the former. a) True b) False	
	3.In the DES algorithm, although the key size is 64 bits only 56 bits are used for the encryption procedure, the rest are parity bits. a) True b) False	
	4.How many rounds does the AES-128 perform? a) 10 b) 12 c) 14 d) 16	
	5.What is the block size in the Simplified AES algorithm? a) 8 Byte b) 40 Byte c) 16 Byte d) 36 Byte	
	6.The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's public key. a) True b) False	
Q 2	1. What is the key size allowed in PGP? a) 1024-1056 b) 1024-4056	**CO1** **1*6**

	c) 1024-4096 d) 1024-2048	
	2.PGP offers _____ block ciphers for message encryption. a) Triple-DES b) CAST c) IDEA d) All of the mentioned	
	3.For digital signatures public key cryptosystem is used. a) True b) False	
	4. The hash function a) Is collision free b) Has manageable collision c) Has high unmanageable level of collision d) None of the mentioned	
	5. The key size of DES is a) 56 bits b) 64 bits c) 128 bits d) 168 bits	
	6.A firewall needs to be _____ so that it can grow proportionally with the network that it protects. a) Robust b) Expansive c) Fast d) Scalable	
Q 3	1.Which component is not included in IP security? a) Authentication Header (AH) b) Encapsulating Security Payload (ESP) c) Internet key Exchange (IKE) d)Handshake Protocol	**CO2** **1*6**
	2. PGP encrypts data by using a block cipher called _____ a) International data encryption algorithm b) Private data encryption algorithm c) Internet data encryption algorithm d) Local data encryption algorithm	
	3._____ provides authentication at the IP level. a) AH b) ESP c) PGP d) SSL	
	4. WPA2 is used for security in _____ a) Ethernet b) Bluetooth c) Wi-Fi d) Email	

	5. What protocol is NOT used in the operation of a VPN? a) PPTP b) IPsec c) YMUM d) L2TP	
	6.AH (Authentication Header) is defined in which of the following standards? a) IPsec b) PPTP c) PPP d) L2TP	
Q 4	1.Which of the following is an advantage of anomaly detection? a) Rules are easy to define b) Custom protocols can be easily analyzed c) The engine can scale as the rule set grows d) Malicious activity that falls within normal usage patterns is detected	**CO3** **1*6**
	2.Which protocol is used to convey SSL related alerts to the peer entity? a) Alert Protocol b) Handshake Protocol c) Upper-Layer Protocol d) Change Cipher Spec Protocol	
	3.Which of the following is not a strong security protocol? a) HTTPS b) SSL c) SMTP d) SFTP	
	4.TSL (Transport Layer Security) is a cryptographic protocol used for securing HTTP/HTTPS based connection. a) True b) False	
	5.HTTPS is abbreviated as _____ a) Hypertexts Transfer Protocol Secured b) Secured Hyper Text Transfer Protocol c) Hyperlinked Text Transfer Protocol Secured d) Hyper Text Transfer Protocol Secure	
	6.In SSL, what is used for authenticating a message? a) MAC (Message Access Code) b) MAC (Message Authentication Code) c) MAC (Machine Authentication Code) d) MAC (Machine Access Code)	
Q 5	1.A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____ a) Chock point b) Meeting point c) Firewall point d) Secure point	**CO4** **1*6**
	2.Network layer firewall works as a _____	

	a) Frame filter b) Packet filter c) Content filter d) Virus filter	
	3.What tells a firewall how to reassemble a data stream that has been divided into packets? a) The source routing feature b) The number in the header's identification field c) The destination IP address d) The header checksum field in the packet header	
	4.Which of the following statements is NOT true concerning VPNs? a) Financially rewarding compared to leased lines b) Allows remote workers to access corporate data c) Allows LAN-to-LAN connectivity over public networks d) Is the backbone of the Internet	
	5.Traffic in a VPN is NOT _____ a) Invisible from public networks b) Logically separated from other traffic c) Accessible from unauthorized public networks d) Restricted to a single protocol in IPsec	
	6.At which two traffic layers do most commercial IDSes generate signatures? a) Application layer and Network layer b) Network layer and Session Layer c) Transport layer and Application layer d) Transport layer and Network layer	
SECTION B		
Q 6	State the key concept of security in using RSA cryptography technique. Explain the parameters on which it differs from AES.	**CO1** **10**
Q 7	Describe Authentication Header (AH) in context of IP Security(IPSec).	**CO2** **10**
Q 8	Describing the role of Hashing technique, compare MD5 and SHA-1 techniques.	**CO3** **10**
Q 9	Explain the SSL protocol stack in brief.	**CO3** **10**
Q 10	Analyze the role of redundant servers in reducing the probability of single point failure. OR Describe the working of VPN that enables an organization to connect its offices at geographical distant location as a part of same LAN using public network.	**CO4** **10**
SECTION-C		
Q 11	Describe the circumstances that mandates the use of different types of Firewalls. Compare the working, capabilities and limitations of Application layer and Network layer firewalls. OR	**CO1** **20**

	Explain below mentioned technologies in context of internet security: a. Message Digest b. Secure Electronic Transaction (SET) c. Deffie-Hellman Algorithm d. Hashed Message Authentication Code (HMAC)	