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.Use Caesar's Cipher to decipher the "HQFUBSWHG WHAW" a) ABANDONED LOCK b) ENCRYPTED TEXT c) ABANDONED TEXT d) ENCRYPTED LOCK	**1*6**
	2.Monoalphabetic ciphers are stronger than Polyalphabetic 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 48bits are used for the encryption procedure, the rest are parity bits. a) True b) False	
	4.How many rounds does the AES-192 perform? a) 10 b) 12 c) 14 d) 16	
	5.What is the block size in the Simplified AES algorithm? a) 8 bits b) 40 bits c) 16 bits d) 36 bits	
	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.Pretty good privacy (PGP) security system uses a) Public key cryptosystem b) Private key cryptosystem	**1*6**

	c) Public & Private key cryptosystem d) None of the mentioned	
	2.PGP offers _____ block ciphers for message encryption. a) Triple-DES b) CAST c) IDEA d) All of the mentioned	
	3.For digital signatures private key cryptosystem is used. a) True b) False	
	4.The digital signature provides authentication to the a) Sender b) Message c) Sender & Message d) None of the mentioned	
	5.Pretty good privacy (PGP) is used in _____ a) Browser security b) Email security c) FTP security d) WiFi security	
	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 included in IP security? a) Authentication Header (AH) b) Encapsulating Security Payload (ESP) c) Internet key Exchange (IKE) d) All of the mentioned	**1*6**
	2.Which mode of IPsec should you use to assure the security and confidentiality of data within the same LAN? a) AH transport mode b) ESP transport mode c) ESP tunnel mode d) AH tunnel mode	
	3._____ provides authentication at the IP level. a) AH b) ESP c) PGP d) SSL	
	4.IP Security operates in which layer of the OSI model? a) Network b) Transport c) Application	

	d) Physical	
	5.Which of the following organizations is primarily concerned with military encryption systems? a) NSA b) NIST c) IEEE d) ITU	
	6.ESP (Encapsulating Security Protocol) 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	**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	**1*6**

	c) Firewall point d) Secure point	
	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 Data Encryption Standards (DES) cryptography. Explain the limitations of DES that leads to the popularity of AES.	**10**
Q 7	Describe the working of Key Management Protocol for IPSec.	**10**
Q 8	Describe the role of Hashed Message Authentication Code Algorithm in securing data.	**10**
Q 9	Explain the progressive steps involved in SSL Handshake Protocol. Describe each step in brief.	**10**
Q 10	Analyze the role of Choke Points in reducing the efficiency of a firewall. OR Describe the technique that enables an organization to connect its offices at geographical distant location as a part of same LAN using public network.	**10**
SECTION-C		
Q 11	List the network issues that recommends the use of different types of Firewalls. Discuss the working, capabilities and limitations of different types of firewalls. OR	**20**

	Explain below mentioned technologies in context of internet security: a. Pretty Good Privacy (PGP) b. Secure Electronic Transaction (SET) c. Deffie-Hellman Algorithm d. Digital Signature	