Duration: 3Hours   [Max Marks : 80]

N.B : (1) Question No 1 is Compulsory.
(2) Attempt any three questions out of the remaining five.
(3) All questions carry equal marks.
(4) Assume suitable data, if required and state it clearly.

1		Attempt any FOUR	[20]
	a	Explain Euclidean Algorithm.	
	b	Explain RC4 stream cipher.	
	c	Differentiate between SHA-1 and MD5	
	d	Explain worms and viruses	
	e	Discuss RSA as a digital signature algorithm.	
2	a	Explain Diffie Hellman key agreement algorithm. Also discuss the possible attacks on it. Consider the example where A and B decide to use the Diffie Hellman algorithm to share a key. They choose p=23 and g=5 as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share	[10]
	b	Explain Advanced Encrypted Standards (AES) in detail.	[10]
3	a	Explain cryptographic hash functions with properties of secure hash function.	[10]
	b	What is ICMP flood attack? Explain in detail.	[10]
4	a	Explain Public Key Distribution in detail.	[10]
	b	Encrypt the string "The Key is hidden under the door" with Play fair cipher using the keyword "domestic".	[10]
5	a	What are the different components of IDS? List and explain different approaches of IDS.	[10]
	b	Explain Needham-schroeder authentication protocol.	[10]
6	a	Write a short note on 1. Packet Sniffing. 2. ARP spoofing.	[10]
	b	Discuss various attacks on Digital signatures.	[10]

Engineeringkeeda.com

X438Y454B4AX438Y454B4AX438Y454B4AX438Y454B4A