[This question paper contains 2 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 3615 **L**

Unique Paper Code : 6202453602

Name of the Paper : INFORMATION SECURITY

Name of the Course : **B.VOC SOFTWARE DEVELOPMENT**

Semester : VI

Duration : 3 Hours

Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. The paper has two sections. Section A is compulsory. Each question is of 5 marks.
3. Attempt any four questions from Section B. Each question is of 15 marks.

Section A			
1	a)	Explain One way hash function.	5
	b)	What is the role of honeypot in network security?	5
	c)	Define Computer Security with its key objectives.	5
	d)	What are vulnerabilities? Explain any two vulnerabilities.	5
	e)	Write down the differences between Active and Passive Attack.	5
	f)	Fill in the blanks: (i) Interruption is an attack on _____. (ii) DES is _____ algorithm. (iii) The SHA-2 family includes several hash functions, such as _____ and SHA-512. (iv) The Diffie Hellman Key exchange allows two parties to securely share a _____ key over an insecure channel. (v) S/MIME uses _____ algorithm for encrypting session keys	5

		Section B	
2	a)	Given the following RSA public key (p=7, q=11), calculate the corresponding private key d and then decrypt the ciphertext C=5.	7
	b)	What is the difference between a Worm and a Bot? Describe how each spreads and the types of damage they can cause to a system or network.	8
3	a)	How to create and use Digital Signatures? Explain its key components. A user receives a Digital Certificate containing: Message (M) = 4, Digital Signature (S) = 16, Certification Authority (CA) public key: e=3 and n=33.Verify whether the certificate is valid using the RSA Algorithm.	7
	b)	Write down the security issues for user authentication.	8
4	a)	Explain how symmetric encryption systems differ from asymmetric encryption systems with suitable examples and block diagrams . Using a simple cipher based on Symmetric Key Cryptography: Encrypt and decrypt the message using an additive cipher: Plaintext: HELLO, Key: 5.	7
	b)	Write short notes on: (a) Spam (b) Digital Certificates (c) Back Door (d) Spoofing	8
5	a)	Describe buffer overflow attack. How attackers take advantage of it, and what are its potential consequences?	7
	b)	What is Heartbeat Protocol? Explain its four general categories to group the attacks.	8
6	a)	Explain the vulnerability of passwords and how can we identify the following attack strategies and countermeasures?	7
	b)	For the Diffie-Hellman key exchange, Alice and Bob agree on a prime number p=23 and a primitive root g=5. Alice's private key is a=6, and Bob's private key is b=15 Compute the shared secret key.	8
7	a)	How do Distributed Denial-of-Service(DDoS) attacks work? Explain common mitigation techniques used to defend against DDoS attacks.	7
	b)	Explain the term 'rootkit' and describe how it compromises a system's security.	8