(b) Define a hash function and its role in message integrity. (5)

[This question paper contains 8 printed pages.]

Your Roll No..............

Sr. No. of Question Paper : 3514 **J**

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 (30 Marks) is compulsory.

3. Attempt any four questions from Section B. Each question is of 15 marks.

4. Use of scientific calculator is allowed.

Section A

1. (a) Explain the utility of substitution boxes in DES. (2)

(b) Define 'attack surface' in the context of computer security. (3)

(c) Explain the concept of CIA Triad in the context of security design principles. (3)

(d) What is the role of a honeypot in network security? (4)

(e) What are the differences between a hash function and a message authentication code (MAC)? (4)

(f) What is a botnet, and how does it use 'zombies' to perform large-scale attacks? (4)

5. (a) What are the primary functions of a firewall? Explain the difference between a packet-filtering firewall and a stateful firewall. (10)

(b) Explain the differences between IPv4 and IPv6 security features. How do these two IP versions handle security differently? (5)

6. (a) How do Distributed Denial-of-Service (DDoS) attacks work? Explain common mitigation techniques used to defend against DDoS attacks. (10)

(b) Explain the term 'rootkit' and describe how it compromises a system's security. (5)

7. (a) Given the following RSA public key (e=3,n=221), calculate the corresponding private key d and then decrypt the ciphertext C=69. (10)

3. (a) Describe the importance of email security and how does Secure/Multipurpose Internet Mail Extensions (S/MIME) ensure email confidentiality and integrity. Provide an overview of how S/MIME works, including its encryption and digital signature process. (10)

(b) What is the role of access control lists (ACLS) in a database management system? Explain how they can be used to enforce security policies. (5)

4. (a) Describe a buffer overflow attack. How attackers take advantage of it, and what are its potential consequences? (10)

(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. (5)

(g) Fill in the blanks: **(5)**

(i) A __________ attack is a large-scale attack involving multiple systems (often compromised) to flood a target system with excessive traffic.

(ii) __________ is a type of malicious software that allows a hacker to remotely control a compromised system.

(iii) DES performs __________ rounds of encryption.

(iv) __________is a type of malware that installs itself on a system and allows remote control by a hacker.

(v) A ____________ is a type of malware that replicates itself to spread to other computers, often without any user intervention.

(h) TRUE/FALSE **(5)**

(i) HTTPS uses SSL and HTTP uses TLS to encrypt data between the client and server.

(ii) Keyloggers are used to track the activity of a system and steal sensitive information like passwords.

(iii) In Public-Key Infrastructure (PKI), digital certificates issued by a Certificate Authority (CA) are used to verify the authenticity of public keys.

(iv) Firewalls can be used to detect, prevent, and respond to network attacks, such as unauthorized access.

(v) A virus requires a host program to execute and propagate itself.

Section B

2. (a) Explain how attack trees can be used to prioritize security measures. Include a detailed explanation of how an attack tree is constructed. (10)

(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. (5)