(iii) Suppose two users have the same password "abc@123". Explain how salting affects their stored hash values.

(iv) Is it safe to store the salt along with the password hash? Justify your answer.

(b) What are the differences among a backdoor, a hot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware? (7.5)

[This question paper contains 8 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 111 **L**

Unique Paper Code : 2342574801

Name of the Paper : Information Security

Name of the Course : **B.A. (P.)**

Semester : VIII

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. **Section A** (Question **1**) is compulsory.
3. Attempt **any 4** questions from **Section B** (Questions **2** to **7**).

Section A

1. (a) Is every threat necessarily an attack? Justify your answer. (3)

(b) Consider the following code fragment: (3)

```
legitimate code
if (date == Friday the 13th);
    crash_computer();
legitimate code
```

What type of malware is this? Give justification for your answer.

(c) What is the difference between a false positive and a false negative in the context of an intrusion detection system? (3)

(d) What do you mean by a digital signature? Provide two examples of digital signature algorithms. (3)

(e) What is meant by 'patching vulnerability' in the context of IoT devices? (3)

(f) Define 'backscatter traffic' and explain its significance in detecting network attacks. (3)

(b) Differentiate between : (2.5×3)

(i) Reactive and Proactive Password Checking

(ii) Access Control List and Capability List

(iii) Active Attacks and Passive Attacks

7. (a) An application stores user passwords in a database using a simple hashing technique : (7.5)

Password → Hash(password)

After a security breach, the developer updates the system to use salting:

Password → Hash(password + salt)

Each user is assigned a unique random salt value, which is stored along with the hash.

(i) Why was storing passwords using only hashing considered insecure in this case?

(ii) How does adding a salt improve password security?

programming practices be applied to address these issues? Illustrate with suitable examples. (7.5)

(b) State and explain any five security threats to wireless networks. (7.5)

5. (a) A small business installs a basic firewall that only filters traffic based on IP addresses and ports but still faces security issues. Identify the type of firewall being used. What are its limitations? Suggest a more advanced firewall type and explain why it would be more effective. (7.5)

(b) Define access control policy. Discuss the four major types of access control policies used in computer security. Are these policies mutually exclusive? Justify your answer. (7.5)

6. (a) An organization is evaluating different cloud options based on cost, control, and security requirements. What are the four cloud deployment models? Explain how each model differs in terms of ownership and usage. (7.5)

(g) Briefly explain the difference between in-band SQL injection and inferential SQL injection attacks. Illustrate each with an example. (3)

(h) What are mutually exclusive role constraints and cardinality constraints in the $RBAC_2$ model? Explain with examples. (3)

(i) What types of programming languages are vulnerable to buffer overflows?

(j) Consider an Automated Teller Machine (ATM) system in which users provide a Personal Identification Number (PIN) and a card to access their accounts. Give one example each of confidentiality, integrity, and availability requirements associated with this system. (3)

Section B

2. (a) A university is launching an online portal where students can log in to access grades, submit assignments, and pay fees. To ensure that students are connecting to the genuine university server

and that their data remains secure, the IT team deploys digital certificates issued by a trusted authority.

With reference to the above scenario, explain what a Public Key Certificate is. Describe its main components and explain how the trusted authority helps in issuing and validating these certificates to ensure secure communication. (7.5)

(b) Briefly explain the different phases in the lifecycle of a computer virus. (7.5)

3. (a) Is symmetric encryption alone suitable for data authentication? If yes, please provide relevant justification. If no, explain the possible security threats associated with using symmetric encryption alone for authentication. Also, suggest a more secure cryptographic mechanism that can be used to ensure authentication. (7.5)

(b) A web application allows users to log in using a username and password. The following code is used to validate user credentials : (7.5)

query = “SELECT *

FROM users

WHERE username = '" + input_username + "'
AND password = '" + input_password + "'; ";

A user enters the following input in the login form:

Username: admin' – –

Password: (left blank)

(i) What will be the final SQL query executed by the system?

(ii) Identify the type of attack being performed.

(iii) Explain how the attack works in this case.

(iv) Suggest any one method to prevent such attacks.

4. (a) A financial web application allows users to input transaction details. During testing, it was observed that unexpected inputs (such as special characters and extremely large values) caused system crashes and inconsistent outputs. How can defensive