

# ***POSSESSION OF MOBILES IN EXAM IS UFM PRACTICE.***

Name J-A.

Enrollment No. 3202

**Jaypee Institute of Information Technology, Noida**

**T1 Examination, Odd 2022**

**B.Tech V Semester**

**Course Title : Fundamentals of Computer Security**

**Maximum Time : 1 hour**

**Course Code : 20B12CS332**

**Maximum Marks : 20**

Course Outcomes		Cognitive Levels
CO1	Explain the fundamental concepts of computer security and malware types	Remember Level(C1)
CO2	Identify types of cryptographic techniques and working of classical cryptosystems	Understand Level(C2)
CO3	Describe authentication and access control paradigms	Understand Level(C2)
CO4	Apply proactive solutions to security like Firewalls and IDS	Apply Level(C3)
CO5	Describe legal and ethical issues with respect to information security	Understand Level(C2)

Q1. You have been tasked with designing an anti-malware for a malware that runs in background and continuously encrypts the files and then asks for a ransom to decrypt. Discuss the design of this anti-malware. What all heuristics/static/dynamic signs you will look for discovering such a malware. Explain each of these signs in detail. [4,CO1]

Q2. Given a network based spreading worm. Explain what all damage such a worm can do on a corporate networks. Which features does a worm exploit to spread laterally? Compare a worm with a Trojan, what is the basic differentiating characteristic between them? Identify the loopholes that each of them exploit to attack? [4,CO1]

Q3. A parasitic virus adds itself to a given executable file. Show how such a virus infects files. You are supposed to list the steps (in pseudo/algorithm form) that such a malware takes. [4,CO1]

**P.T.O**

✓ Q 4. Consider following security breaches and answer which principle of computer security is targeted. Suggest some prevention methods for following breaches: [4,CO1]

✓ a) Consider Veteran's Administration incident in which about 26 million veterans' records were discharged, including name, SSN and Date of Birth. It was stolen from the house of the employee who improperly took the material home.

✓ b) In July 2020, hackers gained access to 130 private and corporate Twitter accounts with at least a million followers each.

✓ c) Suppose an attacker makes an entry in the wrong health record and has the potential of significant consequence.

✓ d) Suppose, the sender send the message and later denies.

✓ Q 5. As a security engineer, you have been given a task to build a system that implement both Bell Lapadula and Biba strict Integrity models. Is it possible especially when a subject would have "high" privilege for BLP and "High" integrity for "BIBA" and an object that such subjects can access have "higher" classification level in BLP and "Higher" integrity level in Biba ("Higher" dominates "high"). Start your answer with either "Yes" or "No" followed by explanation. Also suggest is there any security model that provides above security requirement. [4,CO1]