Question Group A [3 + 2 + 3 + 2 marks] **Question Group B**

1. Users A and B share a secret key. Draw a diagram to illustrate how they can ensure integrity of each other's messages. You are not allowed to use any kind of encryption.
2. What would happen if attackers manage to manipulate a system's certificate store?
3. What methods are available to perform static analysis of malware?
4. In the following scenario, work out the type of malware. State reasons for your classification.

A company experiences system slowdowns and strange network traffic, but security tools detect nothing. Sensitive data is being accessed, yet logs appear clean. The IT team suspects some malware, but traditional detection methods fail, leaving them scrambling to uncover the source of the breach.

1. Draw a diagram to illustrate how a symmetric block cipher can be used to generate a message authentication code (MAC).
2. Give arguments to support or reject the statement: "A certificate should be trusted as long as it is not expired".
3. What methods are available to perform dynamic analysis of malware?
4. In the following scenario, work out the type of malware. State reasons for your classification.

A malicious user installs some malware on a target computer. The malware covertly monitors the user's activities, capturing sensitive information like login credentials and browsing habits. This data is relayed to the attacker, who uses it to compromise accounts and exploit the victim's privacy.

Group A

Q1

They can use prefix MAC, or postfix MAC or prefix-postfix, or even HMAC. Refer to diagram in slides Lec 8 slides 6-7.

Q2

Attackers can install their own root certificate in the system. Then system will start trusting certificates signed by the attacker's rogue certificate authority.

Q3

- Inspecting fie metadata & dependencies
- Inspecting file using hex editor
- Studying code after disassembling

Q4

Rootkit malware because it hides itself very well from logs and other detection methods.

Group B

Q1

Lec 8 slide 4

Q2

Nope, you also need to check if the certificate

(a) is signed by a trusted CA

(b) has not been revoked

Q3

Running the malware inside a sandbox and monitoring

- file, process and system activity
- registry changes
- network traffic

Q4

Spyware because of the private data collection and forwarding that to attacker.