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

1. Using a diagram, illustrate the difference between prefix-hashing and nested-hashing MAC.
2. List the important sections of a digital certificate.
3. As a malware analyst, how would you differentiate between polymorphic and encrypted virus?
4. In the following scenario, work out the type of malware. State reasons for your classification.

A user clicks on a deceptive link in an email, inadvertently installing malware. The infection lies dormant, allowing remote control by hackers. The compromised device begins to send out phishing messages and participate in coordinated attacks, while the user remains unaware of these malicious activities.

1. Draw a diagram to show the steps of digitally signing a piece of data.
2. Discuss the core problem solved by digital certificates.
3. What are the two options for rootkit installation location? Which one is better from an attacker's point of view & why?
4. In the following scenario, work out the type of malware. State reasons for your classification.

A company's network suddenly slows down as multiple computers experience unexpected crashes. Files across the system become corrupted or disappear entirely. The IT team discovers that the infection is spreading rapidly from one machine to another, but traditional defenses are struggling to stop its rapid replication.

Group A

Q1

Lec 8 slides 6 is prefix+postfix

slide 7 is nested hashing.

Q2

- who issued the certificate (CA)
- who the certificate is issued to (subject)
- public key of the owner
- validity period
- digital signature by CA

Q3

I would run the malware is a sandbox and see the structure of new samples it creates after replication. Both mentioned types will have one feature in common: the major chunk of virus body will be random looking data, except for a small part which will contain valid machine instructions. This small part will differentiate between encrypted or polymorphic virus.

- If all the replicated samples share a common piece of code that looks like a decryption loop, it is encrypted virus.
- Otherwise if those instructions are different for each replicated sample, it is polymorphic.

Q4

It is a bot malware because the compromised device has become a part of botnet (participating in coordinated attacks).

Group B

Q1

Lec 8 last slide (left half of diagram)

Q2

When a user presents us their public key, we need to verify if the key really belongs to them or someone else. So, certificates solve the challenge of trust in someone's public key.

Q3

Lec 10 slide 34

From attacker's point of view persistent is better because it is install-only-once effort. OR in-memory is better because it is not detectable by disk scan. *(Either one can be preferred but only with correct argument)*

Q4

It is a worm due to very rapid spread over the network.