Consider a very simple hash function that requires the input to be in decimal digits. For hashing, it sums up all digits in the input, and then performs a modulo 10 division, e.g. H(2458) = 2+4+5+8 mod 10 = 19 mod 10 = 9.

Question Group A

1. Does the above hash function meet 'preimage resistance' requirement? Prove your answer.
2. You receive a message digitally signed by Babar. How would you verify that signature matches the data? Draw a diagram to show the verification steps.
3. As a malware analyst, how would you differentiate between stealth and retro virus?
4. Give arguments to support or reject the statement: "A spyware always creates a backdoor."

Question Group B

1. Does the above hash function meet 'collision resistance' requirement? Prove your answer.
2. Draw a single diagram that shows
   (a) the structure of a public key certificate
   (b) the process of signing it by a certificate authority (CA).
3. Give arguments to support or reject the following statements:
   - Cavity malware is easier to spot than prepending malware.
   - A trojan malware is always a scareware.

[2 + 3 + 3 + 2 marks]

Group A

Q1

Given a hash value, say 5, any number that sums up to 5, 15, 25, ... will be a valid preimage. e.g.

14 (sum=5), 429 (sum=15), 22876 (sum=25)

Since it is quite easy to find preimages, the requirement is not met.

Q2

Lec 8 last slide (right half of diagram)

Q3

I would run the malware is a sandbox and observe its behaviour.

- I would compare the metadata (file size, timestamp, permissions etc.) of files before and after infection. If the metadata remains unchanged but file contents do change (confirmed by comparing hashes), I will conclude it is stealth virus.
- If the malware tries to disable or interfere with the security software (like antivirus), it is a retro virus.

Q4

A spyware collects users' private data or tracks users' activities and sends this information to attackers.

A backdoor, by definition, provides remote access to attackers. This element is not essential for a spyware, so the statement is not true.

Group B

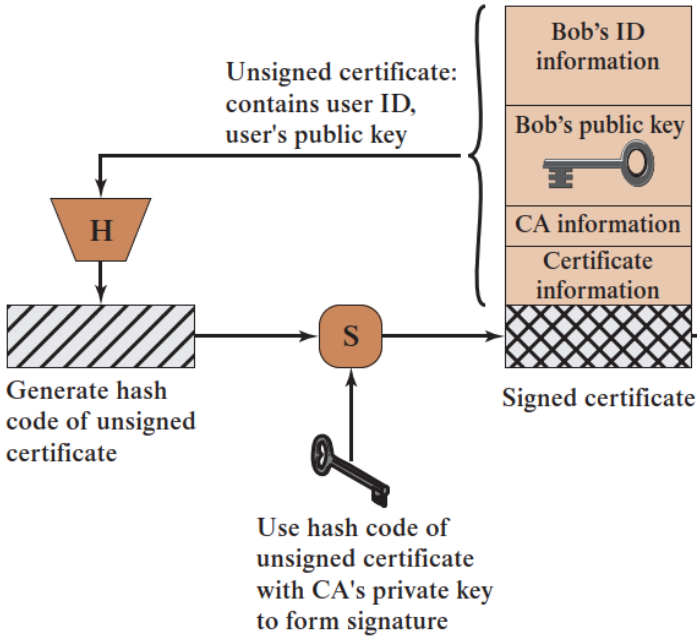
Q1

It is trivial to find two different numbers that hash to same value, e.g.

H(247) = 13 mod 10 = 3, H(21) = 3 mod 10 = 3

Therefore, the function is not collision resistant.

Q2



Q3

i. (3 marks)

Cavity malware is a bit harder to spot than prepending malware since the former keeps the file size unchanged after infection, while the latter will increase file size.

ii. (2 marks)

No, a trojan might be distributed by scaring target users, but could also be presented as a useful utility (without scaring element).