(1) What is “message digest”?

A message digest is a numeric summary (i.e., a checksum) of the message contents (calculated by a specific algorithm, called “hash algorithm”).

(2) If a message digest is attached to a message body, why isn’t “message digest” good enough to prevent “modification of message contents (MIM) attacks”?

A message digest itself is just a number, which can be calculated by anyone, including attackers. Thus, if a message content is modified (or even completely replaced) by an attacker, the attacker can attach his message digest to the modified message. Receivers do not have any way to detect the falsified message digest.

(3) What is “digital signature”?

Digital signature is a message digest encrypted by the sender’s secret (private) key.
(4) Explain how “digital signature” prevents modification of message contents (MIM) attacks.

Digital signatures let receivers detect any unauthorized modifications of message contents. Since digital signatures are encrypted by senders’ secret keys, anyone, except the senders of the messages can correctly encrypt the message digests attached to the message body. Since attackers do not have access to senders’ secret keys, their unauthorized modifications of messages will be always detected by receivers.

(5) What are primary weaknesses in message digests (mention two weaknesses)?

(a) Hash collisions

(b) Neither message digests or digital signatures has a mechanism to prove the correctness (authenticity) of the public keys receivers are supposed to use for decrypting digital signatures signed by senders’ secret keys. After all, they are not a complete solution by themselves.

(6) What is the primary purpose of digital certificate (why we use digital certificate) in network applications?

The primary purpose of digital certificates is prove (i.e., “authenticate”) the ownership of public keys.