7.3.2 Q2 : DS & Hash

Q : ① dimension DS & HD → PKE

②work ?

Solution ① Digital signature and hash digests add authentication , non repudiation and integrity when used with public key encryption.

② The sender encrypts the message using their private key to produce a digital signature

③ To ensure it has not been altered in transit a hash function is used first to creat a digest of the message.