Sample question paper of NETWORK SECURITY

Q1. Which message digest is used as an MDC.
A. keyless
B. keyed
C. either (a) or (b)
D. neither (a) nor (b)

Q2. In _____authentication, the claimant proves that she knows a Secret without actually sending it
A. password-based
B. challenge-response
C. either (a) or (b)
D. neither (a) nor (b)

Q3. A ____ is illicitly introduced code that damages a
A. Protocol
B. Virus
C. Catastrophe
D. Medium

Q4. The _____criterion ensures that we cannot find two messages that hash to the same digest
A. one-wayness
B. weak-collision-resistance
C. strong-collision-resistance
D. none of the above

Q5. In an_____ cipher, a pair of keys is used.
A. symmetric-key
B. asymmetric-key
C. either (a) or (b)
D. neither (a) nor (b)

Q6. The_____ method provides a one-time session key for two parties
A. Diffie-Hellman
B.RSA
C.DES
D.AES

Q7. IPSec uses a set of SAs called the_____
A. SAD
B. SAB
C. SADB
D. none of the above

Q8. ____is actually an IETF version of_____
A. TLS; TSS
B. SSL; TLS
C. TLS; SSL
D.SSL; SLT

Q9. All of the following are examples of real security and privacy threats except:
A. Hackers
B. Virus
C. Spam
D. Worm

Q10. The certificate Authority signs the digital certificate with
A. User's public key
B. User's Private Key
C. It's own public key
D. It's own Private key