MESSAGE AUTHENTICATION CODE.

Select the **most suitable** answer..

1. Another name for Message authentication codes is
a) cryptographic codebreak
b) cryptographic codesum
c) cryptographic checksum
d) cryptographic checkbreak

2. Confidentiality can only be provided if we perform message encryption before the MAC generation.
a) True
b) False

3. Message _____ means that the sender and the receiver expect privacy.

a)confidentiality

b)integrity

c)authentication

d)none of the above

4.Message_____ means that the data must arrive at the receiver exactly as sent.

a)confidentiality

b)integrity

c)authentication

d)none of the above

5. Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.

a)confidentiality

b)integrity

c)authentication

d)none of the above

6. _____ means that a sender must not be able to deny sending a message that he sent.

a)Confidentiality

b)Integrity

c)Authentication

d)Nonrepudiatio

7.Digital signature provides _____.

a)authentication

b)nonrepudiation

c)both (a) and (b)

d)neither (a) nor (b)

8. Digital signature cannot provide _____ for the message.

a)integrity

b)confidentiality

c)nonrepudiation

d)authentication

9. MACs are based on secret _____ keys.

a) Asymmetric

b) Symmetric

10.What is/are the Advantage of Hash Message Authentication Code (HMAC)?

a)HMAC cannot be used if the number of receiver is greater than one.

b)Replay of Message

c)Key Exchange

d)Sometimes need authentication to persist longer than the encryption.