**Tutorial #6**

**Cloud Security INTE2401/2402**

**1. Multiple Choice Questions**

(1) Message Authentication Code (MAC) can be used to achieve \_\_\_\_\_\_\_. D

D

A. Data confidentiality

B. Data integrity

C. Data origin authentication

D. Both B and C

(2) Which of the following approaches in creating a MAC on a message m is insecure? D

D

A. HMAC

B. CMAC

C. CBC-MAC

D. H(k||m), where k is a secret key.

(3) When creating a MAC on a message with HMAC, what is the size of ipad and opad? C

A. 128 bits

B. 256 bits

C. 512 bits

D. 1024 bits

(4) When creating a MAC on a message with HMAC, what is opad? C

A. 3232…3232

B. 3636…3636

C. 5c5c…5c5c

D. 8d8d…8d8d

(5) In CBC-MAC based on AES256, given a message with 100 Mbytes, what is the size of its hash value? B

A. 64 bits

B. 128 bits

C. 160 bits

D. 256 bits

(6) In a network with 20 entities without a trusted third party, how many different secret keys are needed to secure the communication between each pair of the 20 entities? D

A. 19

B. 20

C. 40

D. 190

(7) In simplified Kerberos, the client shares a secret key with \_\_\_\_\_\_\_\_\_ in advance. B

A. The server

B. The authentication server

C. The ticket-granting server

D. The certificate authority

(8) In Simplified Kerberos, there are two types of credentials – ticket and authenticator. Authenticator is generated by \_\_\_\_\_.

A. The client

B. The server

C. The authentication server

D. The certificate authority

(9) In Simplified Kerberos, there are two types of credentials – ticket and authenticator. Tickets are generated by \_\_\_\_\_.

A. The client

B. The server

C. The authentication server

D. The certificate authority

(10) In Simplified Kerberos, the purpose to include the timestamp in Phase 2 is to prevent \_\_\_\_\_\_\_.

A. Eavesdropping attack

B. Modification attack

C. Birthday attack

D. The replaying attack

**2. Conceptual Questions**

Given k= 1234567/K7MDENG+bPxRfiCYEXAMPLEKEY, compute HMAC(k,m), where the message is

AWS4-HMAC-SHA256

20200920M123600Z

20200920/us-east-1/iam/aws4\_request

f536975d06c0309214f805bb90ccff089219ecd68b2577efef23edd43b7e1a59

**3. Programming (HTML and JavaScript) Questions**

Implement the encryption and decryption of AES256 CBC mode.