Roll No. ___________________ Section _________

National University of Computer and Emerging Sciences, Lahore Campus

Course:	**Network Security**	**Course Code:**	**CS411**
Program:	**BS(Computer Science)**	**Semester:**	**Spring 2018**
Duration:	**60 Minutes**	**Total Marks:**	**15**
Paper Date:	**13-April-18**	**Weight**	**15%**
Section:	**-**	**Page(s):**	**04**
Exam:	**Mid-2**		

Instruction/Notes: Attempt all questions in the space provided.

Q 01	Q 02	Q 03	Q 04	Q 05	Total

Question 01: Why is it not a good idea to do keyed hashing in this fashion: h = H(k | message) i.e. the key placed at the start of the message and hashed. (3)

Question 02: ECC uses almost ten times fewer bits in generating a key-size having the same security level as that of RSA. Why is that so? (3)

Question 03: During the establishment of SSL secure communication between a client and a server, the client says hello to the server and the server responds with the certificate that binds its identity to its public key. It may happen so that the server would send more than one certificate to the browser/client. Can you elaborate what other certificates the server would send to the client and what is their purpose?

(3)

Roll No. ___________________ Section _________

Question 04: If the Certification Authority server were to crash, will the network be disabled? If yes/no, why?
(2)

Question 05: Select the correct answer:
(4)

1. **RSA is a ______________________**

   a. **block cipher**
   b. **stream cipher**
   c. **none, because it is not symmetric key encryption**
   d. **A bit of both. It can encrypt any size message.**

2. **The following is not a disadvantage of salt:**

   a. **makes off-line password guessing difficult**
   b. **increases memory requirement**
   c. **makes on-line password guessing difficult**
   d. **decreases memory requirement**

3. **There are _________ functions in MD5:**

    a. **3**
    b. **4**
    c. **5**
    d. **6**

4. **_____________ will add 16 octets of padding no matter what.**

    a. **MD5**
    b. **SHA-1**
    c. **MD2**
    d. **MD4**
    e. **HMAC**

5. **The real problem with using Diffie-Hellman is:**
    a. **Encryption**
    b. **Authentication**
    c. **Integrity of data**
    d. **Spoofing of identity**

6. **The following is true about RSA**
    a. **The block size is fixed**
    b. **The key is larger than the ciphertext**
    c. **The ciphertext is smaller than the plaintext**
    d. **The plaintext is smaller than the key length**

7. **An extension attribute that can be used to find the upper CA in the hierarchy is**
    a. **Signature**
    b. **CA information access**
    c. **Basic constraints**
    d. **Authority information Access**

8. **The main components of PKI are:**
    a. **Certification authority**
    b. **CRL**
    c. **Registration authority**
    d. **Key escrow**