


## National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Network Security	Course Code:	CS411
	Program:	BS (Computer Science)	Semester:	Spring 2018
	Duration:	60 Minutes	Total Marks:	15
	Paper Date:	27-02-2018	Weight	15
	Section:	-	Page(s):	4
	Exam Type:	Final		

**Student : Name:** \_\_\_\_\_ **Roll No.** \_\_\_\_\_

**Section:** ---

Instruction/Notes:

- 1. PLEASE DO NOT WRITE LONG STORIES. BE SPECIFIC!**
- 2. Attempt all questions on the question paper**
- 3. You are not allowed to take any part of the question paper with you**
- 4. You may use rough sheets but you don't need to attach them**

Q.No	Answer
E.g	A
1	
2	
3	
4	
5	

Q.No	Answer
6	
7	
8	
9	
10	

**Q 01: Select the correct option and write them in the table above.**

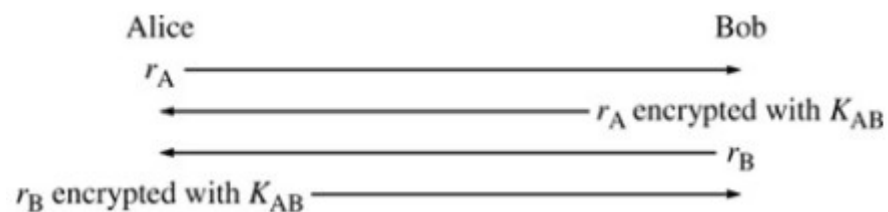
**(10)**

1. An FTP server having an anonymous account used to access files without authentication
  - a. Is a configurational vulnerability
  - b. Is a potential risk
  - c. Is a policy vulnerability
  - d. Is a technological vulnerability
2. The phenomenon with which an attacker is able elevate his access privileges of a resource is called:
  - a. Discretionary access control
  - b. Non-discretionary access control
  - c. Mandatory access control
  - d. Privilege escalation
3. Eavesdropping carried without physically accessing link is termed as
  - a. Tempest
  - b. Electronic emanation
  - c. Wiretapping
  - d. Control zone tapping
4. Your IP address is 125.114.231.123 and you sent a packet with source IP address of 125.114.231.122, you have done

- a. IP snooping
  - b. False IP address injection
  - c. IP spoofing
  - d. IP redirection
5. Hop-by-hop encryption can foil
- a. Traffic padding
  - b. Traffic analysis
  - c. Traffic integrity
  - d. Traffic confidentiality
6. One pillar of security is
- a. Authenticity
  - b. Availability
  - c. Accountability
  - d. Authorization
7. Having a great security policy can ensure security
- a. True
  - b. False
8. A simple DES has
- a. 16 rounds
  - b. 18 rounds
  - c. 20 round
  - d. None of the above
9. Among TCP & UDP which one is considered more secure
- a. TCP
  - b. UDP
  - c. None
  - d. Both are just the same.
10. If the attacker can choose any ciphertext and convert it into plaintext, it is called
- a. chosen plaintext
  - b. chosen ciphertext
  - c. Known plaintext
  - d. Known ciphertext

**Q 02: Instead of using an explicit hashing function like SHA-1, MD5, SHA-2, why can't we use checksum along with a secret code added to it? (3)**

**Q 03: We know that we can use symmetric encryption below to authenticate the other party, do you think hashing can be used in a similar way for authentication? If yes, how? If no, why? Graphical elaborations are always welcomed. (3)**



**Q 04: What are the different security mechanisms that can ensure confidentiality? (2)**

**Q 04: We can create a MAC using an encryption algorithm as well. Why don't we use encryption instead of hashing to compute a MAC? (2)**

**Q 05: What are the two main methods of integrity? Compare the two briefly. (5)**