

UNIVERSITY OF ZULULAND
FACULTY SCIENCE AND AGRICULTURE
DEPARTMENT OF COMPUTER SCIENCE

Assessment IV

COURSE CODE: SCPS 312

Distributed Systems Development

Examiner: Ms I. N. Ezeji

Moderator: Mr. P Tarwireyi

Duration: 55 mins

50 marks

Instructions

1. This paper is *two* (2) pages long.
2. Attempt **all** questions.

1. The University is planning to implement a smart door locking system for the computer labs. The system will allow authorized students and staff to enter the lab while preventing unauthorized individuals from gaining access. The smart door locking system is to be managed remotely, allowing administrators to control access and monitor entry logs in real-time. You are tasked with analysing the security of this system and ensuring it is robust enough to handle potential threats.
 - a. Identify and explain any **two** potential security threats that could affect the smart door locking system in the computer labs. [6]
 - b. Propose **two** possible security policy considerations that can address each of the identified threats from (a). [6]
2. How does the use of encryption techniques such as symmetric and asymmetric cryptography contribute to ensuring confidentiality and integrity in distributed systems? [4]
3. Why is it recommended to use session keys instead of long-lasting keys for confidentiality? [2]
4. What are the two possible implications of joining message 3 and message 4 in the authentication framework shown in **Figure 1**? [4]

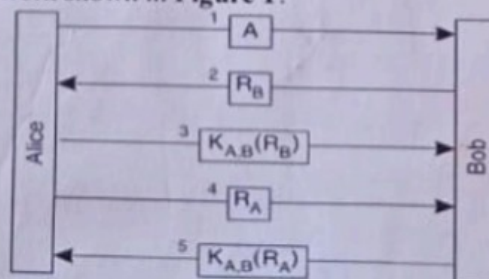


Figure 1

5. Why is it not necessary in Figure 2 for the KDC to know for sure it was talking to Alice when it receives a request for a secret key that Alice can share with Bob?

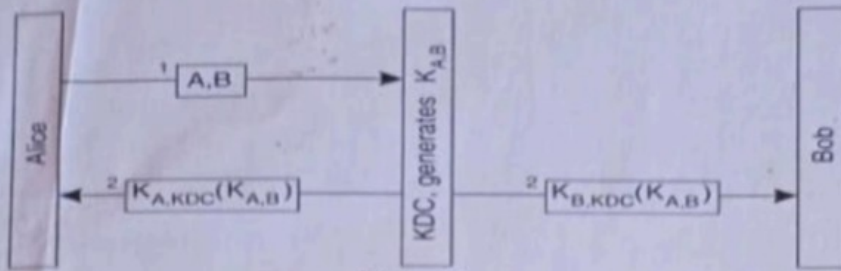


Figure 2

[2]

6. For each of the following scenarios, identify whether it is a Single-Factor Authentication (SFA) or a Multi-Factor Authentication (MFA). Provide explanations for each.
- John logs into his company's email system by entering only his username and password. Sarah logs into her bank account online. [2]
 - Sarah logs into her bank account online. After entering her username and password, she receives a text message on her phone with a verification code. She enters this code to complete the login process. [2]
 - Emily accesses her workplace's secure system using a smart card that she swipes, along with a PIN code she must enter. [2]
7. Figure 3 represent digitally signing a message using public-key cryptography. Explain the process depicted in the Figure 3. [8]

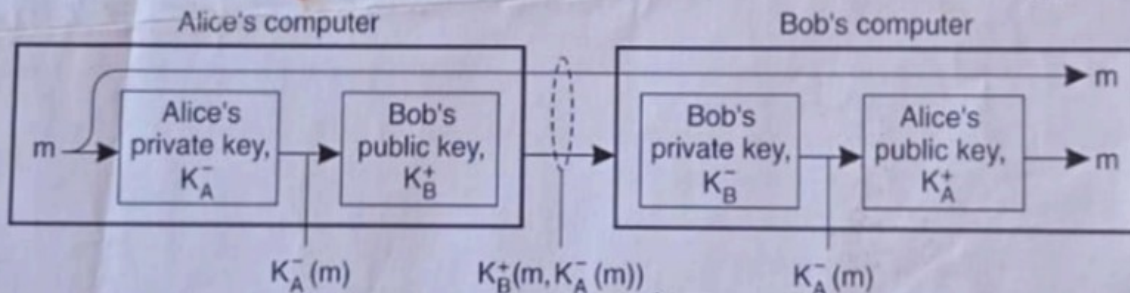


Figure 3

8. The CIA Triad is a guiding model in information security. What does "CIA" stand for? [1]
9. Access rights of objects with reference to subjects are enforced using Access Control Matrix approaches like the Access Control List and Capabilities. Discuss their differences. [3]
10. Discuss any two advantages and two disadvantages of using centralized servers for key management. [8]

All The Best