

UNI CS 3430

Operating Systems

Homework 10

1. Please explain the difference between an access control list and capability list. Which one is typically used for file permissions, and why do you think that is the case?
2. In the following public key encryption scenarios where you are communicating with me, please tell me the secrecy/authentication purpose of the following exchanges.
 - (a) I send you a message: $\text{Encrypt}(\text{KEY}_{\text{sarah_private}}, \text{“Homework is due tomorrow”})$
 - (b) You send me a message: $\text{Encrypt}(\text{KEY}_{\text{sarah_public}}, \text{Encrypt}(\text{KEY}_{\text{my_private}}, \text{“I need another day.”}))$
3. Please come up with a funny/creative scenario similar to the Pentagon Traffic Analysis example where traffic analysis could be used to gain information, even if you can't read the contents of the traffic.
4. Describe one advantage of point-to-point networks over broadcast networks.