Cryptography: Tutorial

Na Yao

February 2017

1. Consider a web mail system. Give examples of security services the system should provide in terms of confidentiality, integrity, authentication and availability.

2. For the system in Question 1, what kinds of threats can you think of? List at least five. Then discuss possible countermeasures you would have. Discuss pros and cons of each countermeasure.

3. What is a brute-force attack? Discuss through an example, taking two situations: one, when the key size is 10 bytes, the other, when the key size is 1 kilo bytes.

4. Research any recent reported example of a significant security breach, focusing on how the breach was achieved, the scale of the breach, the social side of the breach and how do you think the breach can be avoided.