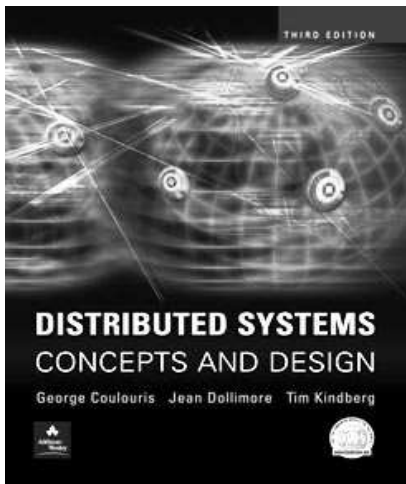


# Exercises for Chapter 7: Security

---



*From* **Coulouris, Dollimore and Kindberg**  
**Distributed Systems:**  
**Concepts and Design**

Edition 3, © Addison-Wesley 2001

# Exercise 7.1

---

⌘ Describe some of the physical security policies in your organization. Express them in terms that could be implemented in a computerized door locking system.

*page 252*

# Exercise 7.2

---

⌘ Describe some of the ways in which conventional email is vulnerable to eavesdropping, masquerading, tampering, replay, denial of service. Suggest methods by which email could be protected against each of these forms of attack

*page 254*

# Exercise 7.3

---

⌘ Initial exchanges of public keys are vulnerable to the man-in-the-middle attack. Describe as many defences against it as you can.

*page 261,298*

# Exercise 7.4

---

⌘ PGP is widely used to secure email communication. Describe the steps that a pair of users using PGP must take before they can exchange email messages with privacy and authenticity guarantees. What scope is there to make the preliminary key negotiation invisible to users? (The PGP negotiation is an instance of the hybrid scheme.)

*page 281,290*

# Exercise 7.5

---

⌘ How would email be sent to a large list of recipients using PGP or a similar scheme? Suggest a scheme that is simpler and faster when the list is used frequently.

*page 290 & Section 4.5*

# Exercise 7.6

---

⌘ The implementation of the TEA symmetric encryption algorithm given in Figures 7.8–7.10 is not portable between all machine architectures. Explain why. How could a message encrypted using the TEA implementation be transmitted to decrypt it correctly on all other architectures?

*page 276*

# Exercise 7.7

---

⌘ Modify the TEA application program in Figure 7.10 to use cipher block chaining (CBC).

*page 273, 276*

# Exercise 7.8

---

⌘ Construct a stream cipher application based on the program in Figure 7.10.

*page 274, 276*

## Exercise 7.9

---

⌘ Estimate the time required to crack a 56-bit DES key by a brute-force attack using a 500 MIPS (million instruction per second) workstation, assuming that the inner loop for a brute-force attack program involves around 10 instructions per key value, plus the time to encrypt an 8-byte plaintext (see Figure 7.14). Perform the same calculation for a 128-bit IDEA key. Extrapolate your calculations to obtain the cracking time for a 50,000 MIPS parallel processor (or an Internet consortium with similar processing power).

# Exercise 7.10

---

⌘ In the Needham and Shroeder authentication protocol with secret keys, explain why the following version of message 5 is not secure:

$$A \rightarrow B: \{N_B\}_{K_{AB}}$$

*page 292*