26. Suppose that when a fingerprint is compared with one other (non-matching) fingerprint, the chance of a false match is 1 in 10^{10}, which is approximately the error rate when 16 points are required to determine a match (the British legal standard). Suppose that the FBI fingerprint database contains 10^7 fingerprints.

    a. How many false matches will occur when 100,000 suspect fingerprints are each compared with the entire database?

    b. For any individual suspect, what is the chance of a false match?

37. Suppose that a particular iris scan systems generates 64-bit iris codes instead of the standard 2048-bit iris codes mentioned in this chapter. During the enrollment phase, the following iris codes (in hex) are determined.

User	Iris code
Alice	BE439AD598EF5147
Bob	9C8B7A1425369584
Charlie	885522336699CCBB

During the recognition phase, the following iris codes are obtained.

User	Iris code
U	C975A2132E89CEAF
V	DB9A8675342FEC15
W	A6039AD5F8CFD965
X	1DCA7A54273497CC
Y	AF8B6C7D5E3F0F9A

Use the iris codes above to answer the following questions.

a. Use the formula in equation (7.1) to compute the following distances:

$$d(\text{Alice}, \text{Bob}), \quad d(\text{Alice}, \text{Charlie}), \quad d(\text{Bob}, \text{Charlie}).$$

b. Assuming that the same statistics apply to these iris codes as the iris codes discussed in Section 7.4.2.3, which of the users, U,V,W,X,Y, is most likely Alice? Bob? Charlie? None of the above?

40. In addition to the holy trinity of "somethings" discussed in this chapter (something you know, are, or have), it is also possible to base authentication on "something you do." For example, you might need to press a button on your wireless access point to reset it, proving that you have physical access to the device.

    a. Give another real-world example where authentication could be based on "something you do."

    b. Give an example of two-factor authentication that includes "something you do" as one of the factors.