Problems

14.1 Show that a random error in one block of ciphertext is propagated to all subsequent blocks of plaintext in PCBC mode (Figure 14.9).

14.2 Suppose that, in PCBC mode, blocks $C_i$ and $C_{i+1}$ are interchanged during transmission. Show that this affects only the decrypted blocks $P_i$ and $P_{i+1}$ but not subsequent blocks.

14.3 The original three-way authentication procedure for X.509 illustrated in Figure 14.6c contains a security flaw. The essence of the protocol is as follows:

$$A \rightarrow B: \ A \{t_A, r_A, ID_B\}$$

$$B \rightarrow A: \ B \{t_B, r_B, ID_A, r_A\}$$

$$A \rightarrow B: \ A \{r_B\}$$

The text of X.509 states that checking timestamps $t_A$ and $t_B$ is optional for three-way authentication. But consider the following example: Suppose A and B have used the preceding protocol on some previous occasion, and that opponent C has intercepted the preceding three messages. In addition, suppose that timestamps are not used and are all set to 0. Finally, suppose C wishes to impersonate A to B. C initially sends the first captured message to B:

$$C \rightarrow B: \ A \{0, r_A, ID_B\}$$

B responds, thinking it is talking to A but is actually talking to C:

$$B \rightarrow C: \ B \{0, r_B, ID_A, r_A\}$$

C meanwhile causes A to initiate authentication with C by some means. As a result, A sends C the following:

$$A \rightarrow C: \ A \{0, r_A, ID_C\}$$

C responds to A using the same nonce provided to C by B.

$$C \rightarrow A: \ C \{0, r_B, ID_A, r_A\}$$

A responds with

$$A \rightarrow C: \ A \{r_B\}$$

This is exactly what C needs to convince B that it is talking to A, so C now repeats the incoming message back out to B.

$$C \rightarrow B: \ A \{r_B\}$$

So B will believe it is talking to A whereas it is actually talking to C. Suggest a simple solution to this problem that does not involve the use of timestamps.

14.4 The 1988 version of X.509 lists properties that RSA keys must satisfy to be secure, given current knowledge about the difficulty of factoring large numbers. The discussion concludes with a constraint on the public exponent and the modulus $n$:

It must be ensured that $e > \log_2(n)$ to prevent attack by taking the $e$th root mod $n$ to disclose the plaintext.

Although the constraint is correct, the reason given for requiring it is incorrect. What is wrong with the reason given and what is the correct reason?