Homework 3
Due at the beginning of class on Oct. 18

Note: The exercises below are from the second edition of the book.

1. Exercise 3.10.
2. Exercise 3.17.

5. In class we discussed the encryption scheme in which a message $m_1, m_2, \ldots$ is encrypted to give
   $$\langle r_1, F_k(r_1) \oplus m_1, r_2, F_k(r_2) \oplus m_2, \ldots \rangle,$$
   where $r_1, r_2, \ldots$ are chosen uniformly at random. This scheme is CPA-secure if $F$ is a pseudorandom function.

   (a) Consider the keyed function $F$ defined by $F_k(r) = k \oplus r$. We showed in class that this $F$ is not a pseudorandom function. Describe how if this $F$ is used in the above encryption scheme, the entire message can be recovered.

   (b) Implement your attack against the ciphertext provided online. (Code for encryption is also provided.)