# Block Ciphers Exercises

P&P, Chapter 2, Exercises 19, 29.
P&P, Chapter 12, Exercises 22, 29.

**A simple block cipher**. Consider the simple block cipher

$$C = (P \oplus K_0) \boxplus K_1$$

where P is the 64-bit plaintext input, $K_0$ and $K_1$ are the two halves of a 128-bit secret key K (i.e. $K_0$ and $K_1$ are each 64 bits and $K = K_0 \,||\, K_1$), and C is the 64-bit ciphertext output. $\oplus$ denotes bit-wise addition modulo two (xor) and $\boxplus$ denotes addition mod $2^{64}$.

*a.* Derive the decryption equation.
*b.* Suppose an adversary acquires two plaintexts P and P' and the corresponding ciphertexts C and C', encrypted with the same key $K = K_0 \,||\, K_1$. Is it possible to solve for $K_0$?

**Decryption with a Feistel Network**. We have stated that Feistel decryption is identical to Feistel encryption, with the subkeys used in reverse order. Prove that Feistel decryption is in fact the inverse of Feistel encryption.

**Nonlinearity of block ciphers**. It has been mentioned that the non-linear components of a block cipher are essential to the cipher's security. Suppose E is a block cipher with a block size of 128 bits, and let E(k, m) denote the encryption of a 128-bit message m using key k. Suppose that E is a linear cipher, meaning that it satisfies the following equation:

$$E(k, m_1 \oplus m_2) = E(k, m_1) \oplus E(k, m_2)$$

As before, $\oplus$ denotes bitwise mod two addition (xor). Suppose an adversary has the ability to carry out a *chosen ciphertext attack:* the attacker can choose some number of ciphertexts $c_1, c_2, \ldots, c_n$ and obtain the corresponding plaintexts $m_1, m_2, \ldots, m_n$ (so $c_1 = E(k, m_1)$, $c_2 = E(k, m_2)$, …, $c_n = E(k, m_n)$). Can the adversary recover the secret key k? If so, what is the minimum number of chosen ciphertext / plaintext pairs required.

**Block cipher modes and bit errors.** Suppose a message is encrypted with a block cipher in one of the modes discussed in class (ECB, CBC, CFB, or CTR) and during transmission of the message, a bit error occurs (that is, a single bit value within the message is changed). Which and how many blocks will be corrupted in the decrypted message?

**Which block cipher mode to use?** For each of the following scenarios, determine which of the four block cipher modes discussed in class would be most appropriate. Justify your answer.

a. Encryption of the social security number field within every record of a database.
b. Encryption of a Word document (.doc) that will be sent as an email attachment.
c. Sector-by-sector encryption of an external hard drive.
d. Real-time encryption of a non-packetized bit stream (e.g. raw digital video).
e. Suppose a communication system encrypts data using AES-128 and has the ability to update keys over the network; that is, when a node on the network needs to update its key, a network controller can send the node a new key *encrypted with the current key*. What block cipher mode would me most appropriate when encrypting the new key to send to the node?