Problems from Trappe/Washington Book:
Chapter 4: 1, 3, 4, 5

Supplemental Problems:
1. In problem 5 of Chapter 4, you showed that $K = 11 \cdots 1$ (56 bits) was a weak key of DES since $E_K(E_K(m)) = m$. If we insert parity bits to represent $K$ using 64-bits, what would the hexadecimal notation for the parity-bit expanded representation of $K$?

2. The cipher block chaining (CBC) mode has the property that it recovers from errors in ciphertext blocks. Show that if an error occurs in $C_j$, then this only affects two blocks for decryption. Which two blocks?