Symmetric encryption ungraded homework

This homework is ungraded. Its purpose is to help you understand course material. Doing these problems may help you with your graded homework and quiz. Problems like these may appear on the midterm or final. You should attempt to complete them before the end of the module (time permitting), and at a minimum study them and their provided solutions.

1. GF(16) is defined like GF(256) except the polynomials all have degree less than 4 and the modulus is $x^4 + x + 1$. Calculate the following, each digit representing a field element in hexadecimal. (a) 5+F. (b) 5-F. (c) 5·F. (d) 5/F. Note that 5-F is shorthand for 5+(-F) where -F is F's additive inverse, and 5/F is shorthand for $5 \cdot F^{-1}$ where F^{-1} is F's multiplicative inverse.
2. The AES S-box found on Page 101 of the *Understanding Cryptography* reading is a permutation, and therefore could be used in the modes of operation we learned (ECB, CBC, CTR, OFB). Use the S-box in each of the modes to encrypt "abc" (search the internet for "ASCII table" to find the binary representation of a, b, and c). In modes that need padding use 10^* padding. For modes that need an IV use 01010011. For modes that need a nonce, use 0110. Note that the S-box would never be used this way, I'm just using it as a readily available permutation for practice.
3. Let's say that a ciphertext that was created using a mode-of-operation has a single bit toggled in it's i-th block before decryption. How damaging is it to the decryption? Describe the damage with respect to errors in the resulting plaintext blocks (eg, "plaintext block i has a single bit error", or "all plaintext blocks later than i look random", etc). Do this for each of the modes ECB, CBC, CTR, OFB.
4. Let's say that the key used with AES-128 is `0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F`. Compute the first two round keys used by AES-128 in this case (ie, compute k_0 and k_1 in Fig 4.2 which is also W[0] through W[7] in the Fig 4.5).
5. Using the k_0 and k_1 computed in Problem 1, what is the value of the evolving AES block after "round 1" in Fig 4.2 if initially the AES block ("plaintext x" in Fig 4.2) is `0xFF, 0xFE, 0xFD, 0xFC, 0xFB, 0xFA, 0xF9, 0xF8, 0xF7, 0xF6, 0xF5, 0xF4, 0xF3, 0xF2, 0xF1, 0xF0`?
6. *Cryptography Engineering* Exercises 3.1, 4.1, 4.3 and 4.6.

Ungraded homework solutions

These are best studied after completing the homework or after struggling with it for a while.

Solutions PDF.