Symmetric encryption homework MM - Do before mid-module quiz

The ungraded homework assigned below is never turned in, but should be completed before the mid-module quiz opens.

The graded homework assigned below is due 24 hours before the mid-module quiz opens. No late graded homework is accepted.

The mid-module homework can be done individual or collaboratively. Read the collaboration policy to know what this means.

Ungraded homework

The point of ungraded homework is to develop your abilities and prepare you for the quiz. Solutions will be provided, but they should be consulted only when you need a hint and/or afterward to compare and contrast your solution with mine.

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". 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. *Cryptography Engineering* Exercises 3.1, 4.1, 4.3 and 4.6.

Ungraded homework solutions

Study these only after completing the homework or after struggling with it for a while.

Solutions

Graded homework

On Canvas an Old MM Quiz for this module will appear soon. Complete the quiz before it closes.

Each old quiz is worth 1% of your overall grade. It is untimed and you may take it as many times as you want. You may do it alone or in collaboration. It is intended as a warm-up for the actual quiz.