Symmetric encryption homework EOM - Do before end-of-module quiz

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

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

The end-of-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. 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).
2. 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`?

Ungraded homework solutions

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

Solutions pdf

Graded homework

1. On Canvas an Old EOM Quiz for this module will appear soon. Complete the quiz before it closes, 24 hours before the end-of-module quiz opens.

   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.

2. On Mimir a programming assignment for this module will appear soon. Complete the assignment before it closes, 24 hours before the end-of-module quiz opens.