Assignment # 3

Homework

Homework problems are a preparation for the quizzes. They are *not* graded. Please use the `piazza` forum to post questions you have on these problems.

- 4.3, 4.4, 4.5, 4.9, 4.10, 4.16, 5.2, 5.3, 5.10

Project

Note: For submissions on `mywpi`: Please submit a single pdf file containing your results. Please submit source code as a separate file, but make sure to have it listed in the pdf as well.

1. Compute in $GF(2^8)$:

   $$(x^6 + x^5 + x + 1)/(x^7 + x^6 + x^4 + 1)$$

   where the irreducible polynomial is the one used by AES, $P(x) = x^8 + x^4 + x^3 + x + 1$. Note that Table 4.2 contains a list of all multiplicative inverses for this field. Please show all intermediate steps.

2. Consider a modified substitution-permutation network where instead of carrying out the key-mixing, substitution, and permutation steps in alternating order for r rounds, the cipher instead first applies r rounds of key-mixing, then carries out r rounds of substitution, and finally applies r permutations. Analyze the security of this construction.

3. As is often true in cryptography, it is easy to weaken a seemingly strong scheme by small modifications. Assume a variant of the OFB mode by which we only feed back the 8 most significant bits of the cipher output. We use AES and fill the remaining 120 input bits to the cipher with zeros.

   (a) Draw a block diagram of the scheme.

   (b) Why is this scheme weak if we encrypt moderately large blocks of plaintext, say 100 kByte? What is the maximum number of known plaintexts an attacker needs to completely break the scheme?

   (c) Let the feedback byte be denoted by FB. Does the scheme become cryptographically stronger if we feedback the 128-bit value $FB, FB, \ldots, FB$ to the input (i.e., we copy the feedback byte 16 times and use it as AES input)?

   (d) Replace the original zero padding of the encryption scheme described above with a new padding scheme that restores the secrecy requirement. Which essential property do you need to add to the encryption scheme?

4. The goal of this problem is to encrypt the payload of a .bmp file using three different modes of operation. The cipher to be used is AES. As in the last project, please use a preexisting AES implementation for this project. The .bmp picture `Gompei.bmp` as well as code for opening, reading and writing a .bmp file in Python and sage are provided.

   Please write code to encrypt the payload of `Gompei.bmp` using AES in (*i*) electronic codebook (ECB) mode (*ii*) cipher block chaining (CBC) mode and (*iii*) counter (CTR) mode of operation. Submit the code in each case together with the encrypted file. The key (and initialization vector (IV)) should be all-zero.

Good Luck and Have Fun!