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.

- 4.4, 4.5, 4.9, 4.10, 5.1, 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. 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.

2. A small company has developed a messaging application that allows to send text messages between two parties. The transferred messages m are encoded in the ASCII format, i.e., each symbol m_i of the message $M = m_0\, m_1 \ldots m_l$ (be it a letter, a number, or other symbol) is represented by a string of 7 bits, i.e., $|m_i| = 7\,\text{bit}$.

   At some point the company decides to add security to the application by encrypting the transferred messages. For this, sender and receiver share a secret key k via a secure channel. The company decides to use the highly secure AES-256 encryption scheme for marketing reasons. The implemented encryption scheme takes each symbol m_i and encrypts it separately. Missing input bits are padded with zeros 0^{121}. The resulting encryption scheme is:

$$\begin{aligned} c_i &= AES_k(m_i||0^{121}) \\ C &= c_0\, c_1 \ldots c_l \end{aligned}$$

   (a) Is this encryption scheme secure? How many different ciphertext symbols does this scheme produce? Describe an efficient attack against this encryption scheme. What does an adversary need to successfully perform your attack?

   (b) Does your attack recover the secret key? What is the attack complexity to recover the secret key?

The company asks you to improve the employed encryption scheme. Unfortunately you may not change the main protocol (the product is in use and being advertised as highly secure AES-based messenger). Each symbol m_i still has to be encrypted separately.

(c) Replace the 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?

3. 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!