IT-Security Cryptography and Secure Communications

Excercise: **AES**

Lecturer: *Prof. Dr. Michael Eichberg*

Version: 2023-10-12

For this exercise let's assume that we have a 128 bit key.

1. RoundKey computation:

   Given the following RoundKey:

   $rc_1 = w[4] || w[5] || w[6] || w[7] =$

   ```
   -w[4]------   -w[5]------   -w[6]------   -w[7]------
   E2 32 FC F1   91 12 91 88   B1 59 E4 E6   D6 79 A2 93
   ```

   Calculate rc_2; i.e. the Roundkey for the second round.

   1. Before performing the concrete computation, first write down the formulae:

      $w[8] = \ldots \oplus \ldots$

      $w[9] = \ldots \oplus \ldots$

      $w[10] = \ldots \oplus \ldots$

      $w[11] = \ldots \oplus \ldots$

   2. Calculate *w[8]* and *w[9]*.

2. Let's assume that the current State matrix is:

   ```
   00 3C 6E 47
   1F 4E 22 74
   0E 08 1B 31
   54 59 0B 1A
   ```

   Perform the step *substitute bytes*; i.e., apply the s-box transformation.

3. Perform the *shift rows transformation* on your previous result.

4. Given the following State matrix:

   ```
   6A 59 CB BD
   4E 48 12 A0
   98 9E 30 9B
   8B 3D F4 9B
   ```

   Perform the mix columns transformation for the missing field ($S'_{0,0}$):

```
?? C9 7F 9D
CE 4D 4B C2
89 71 BE 88
65 47 97 CD
```

5. Apply the RoundKey:

   ```
   -w[x]------   -w[x+1]----   -w[x+2]----   -w[x+3]----
   D2 60 0D E7   15 7A BC 68   63 39 E9 01   C3 03 1E FB
   ```

   to the State:

   ```
   AA 65 FA 88
   16 0C 05 3A
   3D C1 DE 2A
   B3 4B 5A 0A
   ```

6. Ask yourself what happens if you encrypt a block just consisting of `0x00`s with a key also consisting only of `0x00`s?