Homework 8 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

15.12.2009

Exercise 22.

Within the step `MixColumns` of the AES algorithm a vector $\mathbf{r}$ is given by $\mathbf{r} = \mathbf{Tc}$ with $\mathbf{c} = (c_0, c_1, c_2, c_3)'$, $c_i \in \mathbb{F}_{2^8}[x]$, and

$$T = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix}.$$

Show $(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) = r_3u^3 + r_2u^2 + r_1u + r_0 \mod u^4 + 1$.

Exercise 23.

Consider the block cipher of block length 3 given by the permutation

$$\pi = (1\ 2\ 3).$$

A bit block $b_1b_2b_3$ of length 3 is encrypted as follows:

$$e_\pi(b_1b_2b_3) = b_{\pi(1)}b_{\pi(2)}b_{\pi(3)} = b_2b_3b_1.$$

Encrypt the message 101001110 in ECB-, CBC-, OFB- and CFB-mode. Use $C_0 = 101$ as initial vector.

Exercise 24.

A sequence of message blocks is encrypted with AES in the modes ECB, CBC, OFB, CFB, and CTR.

(a) During transmission exactly one bit changes. How many bits are decrypted wrongly at maximum?

(b) What happens, if one bit of the ciphertext is lost or an additional one is inserted?