

Homework 8 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer
06.01.2009

Exercise 23. Within the step `MixColumns` of the AES algorithm a vector \mathbf{r} is given by $\mathbf{r} = \mathbf{T}\mathbf{c}$ 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 $(c_3u^3 + c_2u^2 + c_1u + c_0)((x+1)u^3 + u^2 + u + x) = r_3u^3 + r_2u^2 + r_1u + r_0 \pmod{u^4 + 1}$.

Exercise 24. A sequence of message blocks is encrypted with AES in the modes ECB, CBC, OFB, CFB, and CTR.

- During transmission exactly one bit changes. How many bits are decrypted wrongly at maximum?
- What happens, if one bit of the ciphertext is lost or an additional one is inserted?

Exercise 25. Let $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ be the Euler φ -function, i.e. $\varphi(n) = |\mathbb{Z}_n^*|$.

- Determine $\varphi(p)$ for a prime p .
- Determine $\varphi(p^k)$ for a prime p and a positive integer k .
- Determine $\varphi(pq)$ for two different primes $p \neq q$.
- Determine $\varphi(4913)$ and $\varphi(899)$.

Christmas Exercise.

TEDDCTYPKZ KUSLMNVAUD PWYCTULIWP

