Homework 6 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

06.12.2013

Exercise 15. A sequence of message blocks is encrypted with AES in the modes ECB, CBC, OFB, CFB, and CTR. The ciphertext is sent from Alice to Bob over a channel with random transmission errors.

(a) Bob wants to decrypt the ciphertext. Assume that exactly one bit in one block of the ciphertext changes during transmission. How many bits are wrongly decrypted in the worst case?

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

Exercise 16.

Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$.
Furthermore, let $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$. Prove that

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Exercise 17. Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$.

(a) Determine $\varphi(p)$ for a prime p.

(b) Determine $\varphi(p^k)$ for a prime p and $k \in \mathbb{N}$.

(c) Determine $\varphi(p \cdot q)$ for two different primes $p \neq q$.

(d) Determine $\varphi(4913)$ and $\varphi(899)$.