Exercise 7 in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-06-18

Problem 20. *(Operation Modes)* 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?

Problem 21. (*proof Euler's theorem*) 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

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

Problem 22. *(Miller-Rabin Primality Test)*

a) Use the Miller-Rabin Primality Test to prove that 341 is composite.

b) The Miller-Rabin Primality Test comprises a number of successive squarings. Suppose a 300-digit number n is given. How many squarings are needed in worst case during a single run of this primality test?

Problem 23. *(Proof Chinese Remainder Theorem)*
Prove the Chinese Remainder Theorem: Suppose $m_1, \dots, m_r$ are pairwise relatively prime, $a_1, \dots, a_r \in \mathbb{N}$.

The system of r congruences

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, \dots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x \equiv \sum_{i=1}^{r} a_i\, M_i\, y_i \pmod{M},$$

where $M_i = M/m_i$, $y_i = M_i^{-1} \pmod{m_i}$, $i = 1, \dots, r$.