Homework 9 in Cryptography I

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

22.12.2009

Exercise 25.

Besides the CBC mode, the CFB mode can be used for the generation of a MAC. The plaintext consists of the blocks $M_1, ..., M_n$, and we set the initialization vector $C_0 := M_1$. Now, we encrypt $M_2, ..., M_n$ in CFB mode with the key K, which results in the ciphertexts $C_1, ..., C_{n-1}$. For the MAC, we use $MAC_K := E_K(C_{n-1})$.

Show that this scheme results in the same MAC as the algorithm in example 10.5 from the lecture notes with the initial value set to $C_0 := \mathbf{0}$.

Exercise 26.

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

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

Exercise 27.

Pierre de Fermat is said to have factored numbers n by decomposing them as

$$n = x^2 - y^2 = (x - y)(x + y).$$

Use this method to factor the integer $n = 13199$. Describe an algorithm to determine the above x and y. Can this method be applied in general for any n?