Homework 7 in Cryptography I

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

16.12.2008

Exercise 19. A block cipher is a cryptosystem where plaintext and ciphertext space are the set $\mathcal{A}^n$ of words of length n over an alphabet $\mathcal{A}$. The number n is called the block length.

Show that the encryption functions of block ciphers are permutations. How many different block ciphers exist if $\mathcal{A} = \{0, 1\}$ and the block length is $n = 6$?

Exercise 20. The ring $\mathbb{Z}_2$ is a field that is also named $\mathbb{F}_2$. The ring $\mathbb{Z}_4$ is not a field, but there exists a field $\mathbb{F}_4$ with 4 elements. This field can be constructed as the residue class ring of the polynomial ring $\mathbb{F}_2[x]$ modulo the ideal generated by $f := x^2 + x + 1$. Specify all elements of the field $\mathbb{F}_4$ and determine the addition und multiplication tables for $\mathbb{F}_4$.

Exercise 21. Consider the finite field $\mathbb{F}_4$ from Exercise 20. Construct an extension field $\mathbb{F}_{16}$ of $\mathbb{F}_4$ with 16 elements and describe your approach.
Hint: Start with the polynomial ring $\mathbb{F}_4[U]$.

Exercise 22. Consider the following AES-128 key given in hexadecimal notation:

$$K = 2d\ 61\ 72\ 69\ 65\ 00\ 76\ 61\ 6e\ 00\ 43\ 6c\ 65\ 65\ 66\ 66$$

a) What is the round key K_0?

b) What are the first 4 bytes of round key K_1?