Cryptography

PRIV.-DOZ. DR. ADRIAN SPALKA, KONSTANTIN ZIEGLER

3 Assignment

(Due: Thursday, 18 November 2010, 12^{00})

Exercise 3.1. (7 points) Design a protocol to

(i) agree over the phone on a “random” bit,

(ii) play rock-paper-scissors over a chat-channel.

Comment on correctness and completeness.

Exercise 3.2 (DAC vs. MAC)**.** (7 points) How can you transfer the information of the control matrix in a DAC into the partially-ordered set of a MAC. How can you go back? What is the blow-up in both directions?

Exercise 3.3 (The finite field $\mathbb{F}_{256}$)**.** (6 points) The finite field of 256 elements plays a central role in the description of AES. Its elements are polynomials of degree less than 8 with coefficients in the two-element field $\mathbb{F}_2$. Each element is of course given by eight bits, which we can also read as a hexadecimally written byte, so that, for example, $x^7 + x^4 + 1$ is given by (10010001), which can be read as `91`. Addition and multiplication in the field are the usual addition and multiplication of polynomials, apart from the rule, that the result is reduced modulo the polynomial $x^8 + x^4 + x^3 + x + 1$. Carry out the following computations and document your intermediate steps:

(i) Add $x^5 + x + 1$ and $x^7 + x^6 + 1$.

(ii) Add `23` and `C1`.

(iii) Multiply $x^5 + x + 1$ and $x^7 + x^6 + 1$.

(iv) Multiply `23` and `C1`.

(v) Calculate the inverse of $x^4 + x^3 + x^2 + x + 1$.

(vi) Calculate the inverse of `23`.

Exercise 3.4 (mathematical bonus)**.** (+2 points) Why is there no field with six elements?