Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

0. Repetition sheet

Exercise 0.1 (High powers). *Compute* $3^{98765432101}$ *in* $\mathbb{Z}_{101}$.

Exercise 0.2 (Touching $\mathbb{F}_4$). *Consider polynomials of degree less than* 2 *over the field* $\mathbb{F}_2$. *Define addition and multiplication of them modulo the polynomial* $X^2 + X + 1$.

(i) Write down the complete list of elements.

(ii) Write down the addition table.

(iii) Write down the multiplication table.

We can now consider polynomials over $\mathbb{F}_4$: $T^2 + T + 1$ *is such a polynomial. Factor it (over* $\mathbb{F}_4$*).*

Exercise 0.3 (Computing in $\mathbb{F}_{256}$). *Let* M *be your student id. Let*

$$a = M \bmod 256, b = (M \operatorname{div} 256) \bmod 256, \text{ and } c = (a + b) \bmod 256$$

Now interpret a, b *and* c *as elementes of* $\mathbb{F}_{256}$. *Compute in* $\mathbb{F}_{256}$

(i) $a + b$ *(Attention! Usually the result will not be* c*!),*

(ii) $a \cdot b$, *and*

(iii) $1/a$ *(or* $1/b$ *in case* $a = 0$*).*

Note*: If* $x = x_1 \cdot 256 + x_0$ *with* $0 \leq x_0 < 256$, *then* $x \operatorname{div} 256 = x_1$ *and* $x \operatorname{rem} 256 = x_0$.

Exercise 0.4 (Computing inverses). *If possible compute the inverse*

(i) ... of 89 *in the ring* $\mathbb{Z}_{101}$,

(ii) ... of 42 *in the ring* $\mathbb{Z}_{1001}$,

Give a proof if no inverse exists.