Summer School
crypt@b-it 2008

JÉRÉMIE DETREY, DANIEL LOEBENBERGER, MICHAEL NÜSKEN

1. Preparation sheet

Exercise 1.1 (A family of groups).

Consider the group $\mathbb{Z}_p^\times$ of units modulo a prime p. [Think of it as an object oriented class consisting of the integers $1, 2, \ldots, p-1$ with a method for multiplying two of them. The product is the integer product reduced modulo p. Eg. $4 \cdot 5 = 6$ in $\mathbb{Z}_7^\times$. This definition works for any number $p \in \mathbb{N}_{\geq 2}$, whether p is prime or not.]

(i) Calculate the product of 13 and 17 in $\mathbb{Z}_{29}^\times$.

(ii) Calculate the inverse of 12 in $\mathbb{Z}_{29}^\times$. [...and explain how to do that in general. Brute force is no solution!]

(iii) Check that $a^{28} = 1$ in $\mathbb{Z}_{29}^\times$ for any $a \in \mathbb{Z}_{29}^\times$. [This is an instance of Fermat's little theorem.]

(iv) Compute $2^{1\,234\,567}$ in $\mathbb{Z}_{29}^\times$. Use as few multiplications in $\mathbb{Z}_{29}^\times$ as possible; explain.

(v) Find the *discrete logarithm* x such that $2^x = 17$ in $\mathbb{Z}_{29}^\times$.

In general the discrete logarithm problem is considered to be difficult. No general polynomial time solution is known at present.

(vi) The baby-step, giant-step method finds a discrete logarithm in $\mathbb{Z}_p^\times$ with only $\mathcal{O}(\sqrt{p})$ operations. [Note that this is *not* polynomial in the input size, which is $\Theta(\log p)$.] Given $a, b \in \mathbb{Z}_p^\times$ the problem is to find $x \in \mathbb{Z}_{p-1}$ such that $a^x = b$ in $\mathbb{Z}_p^\times$. Proceed as follows: Split the unkown $x = x_1 r + x_0$ with $r = \lceil \sqrt{p} \rceil$, $0 \leq x_0 < r$. Note that $0 \leq x_1 < \frac{p}{r}$. [Prove this!] Now compute the *giant steps* $a^{x_1 r}$ for all possible values of x_1, and the *baby steps* $a^{-x_0} b$ for all possible values of x_0.

- Prove that $a^{x_1 r} = a^{-x_0} b$ if and only if x is a solution to the equation $a^x = b$ in $\mathbb{Z}_p^\times$.
- Show that you only need at most $\mathcal{O}(\sqrt{p})$ operations (and memory) to find x_1 and x_0.

Actually, one can show that for a 'generic' group (of prime order) this is close to optimal. Yet, the groups $\mathbb{Z}_p^\times$ are not generic and faster algorithms exist.

(vii) Reconsider $2^x = 17$ in $\mathbb{Z}_{29}^\times$. The equation implies that

$$2^{4x} = 17^4 \qquad\qquad 2^{7x} = 17^7.$$

Since $2^{28} = 1$ in $\mathbb{Z}_{29}^\times$ the left equation determines x only modulo 7 whereas the right one determines x modulo 4. Baby-step giant-step needs only "$\mathcal{O}(\sqrt{7})$" operations [Why the quotes?] to find that $x = 0$ in $\mathbb{Z}_7$ [ie. $2^{4 \cdot 0} = 17^4$] and "$\mathcal{O}(\sqrt{4})$" operations $x = 1$ in Z_4 [ie. $2^{7 \cdot 1} = 17^7$].

Use the Chinese Remainder Theorem to determine x in $\mathbb{Z}_{28}$ and compare to your previous solution of $2^x = 17$ in $\mathbb{Z}_{29}^\times$.

Exercise 1.2 (Finite fields).

We consider here the set of binary polynomials $\mathbb{Z}_2[x]$, where $\mathbb{Z}_2 = \{0, 1\}$ is the set of integers modulo 2.

(i) What is the algebraic structure of $\mathbb{Z}_2[x]$?

In order to bound the number of elements in this set, we restrict ourselves to polynomials of degree at most 2. We note this set as $\mathbb{Z}_2[x]^{(\leq 2)}$. We transparently represent each polynomial $a(x) = a_2x^2 + a_1x + a_0$ as the bit-string $a_2a_1a_0$. For instance, 110 represents the polynomial $x^2 + x$.

(ii) How many elements are there in this set? List them.

(iii) Describe how to compute the sum $c(x)$ of two polynomials $a(x)$ and $b(x) \in \mathbb{Z}_2[x]^{(\leq 2)}$. Give the corresponding addition table.

(iv) We now consider multiplication over this set. What is the degree of the product $c(x)$ of two polynomials $a(x)$ and $b(x) \in \mathbb{Z}_2[x]^{(\leq 2)}$? Does $c(x)$ still lie in $\mathbb{Z}_2[x]^{(\leq 2)}$?

(v) Describe a way of "trimming" $c(x)$ so that the result of a multiplication actually remains in $\mathbb{Z}_2[x]^{(\leq 2)}$.

Taking $f(x) = x^3 + x + 1$, which can be shown to be irreducible over $\mathbb{Z}_2$, we consider $\mathbb{Z}_2[x]/(f(x))$, that is the set of binary polynomials modulo $f(x)$.

(vi) Show that $\mathbb{Z}_2[x]/(f(x))$ and $\mathbb{Z}_2[x]^{(\leq 2)}$ contain exactly the same elements.

(vii) Give the multiplication table over $\mathbb{Z}_2[x]/(f(x))$.

(viii) Verify from that table that every element $a(x) \in \mathbb{Z}_2[x]/(f(x))$, $a(x) \neq 0$, has a multiplicative inverse $a^{-1}(x)$. Could we have expected that?

(ix) What is the algebraic structure of $\mathbb{Z}_2[x]/(f(x))$?

Now let's see what happens if we choose another irreducible polynomial of degree 3. Namely, we take $g(x) = x^3 + x^2 + 1$.

(x) Verify that the element $y(x) = x + 1 \in \mathbb{Z}_2[x]/(f(x))$ is a solution of the equation $g(y) = y^3 + y^2 + 1 = 0$.

(xi) Consider the set of binary polynomials in the variable y, modulo $g(y)$, noted $\mathbb{Z}_2[y]/(g(y))$. Express all the elements of this set in function of x.

Remark that each element $a(y)$ of $\mathbb{Z}_2[y]/(g(y))$ can be mapped to an element $b(x) = a(x+1)$ of $\mathbb{Z}_2[x]/(f(x))$. We note φ this mapping.

(xii) Given two polynomials $a(y)$ and $b(y) \in \mathbb{Z}_2[y]/(g(y))$, verify that $\varphi(a + b) = \varphi(a) + \varphi(b)$, where the first addition is performed over $\mathbb{Z}_2[y]/(g(y))$ whereas the second one is performed over $\mathbb{Z}_2[x]/(f(x))$.

(xiii) Same question for the multiplication.

(xiv) Conclude.

Actually, one can show that finite fields like $\mathbb{Z}_2[x]/(f(x))$ are unique up to isomorphism. The choice of the irreducible polynomial only impacts on the representation of the elements, but not on the intrinsic algebraic structure of the set. This is why we will usually note it simply $\mathbb{F}_{2^3}$ or $\mathbb{F}_8$. It is an extension of degree 3 of $\mathbb{Z}_2$, which is itself the finite field $\mathbb{F}_2$.

Exercise 1.3 (Computing in $\mathbb{F}_{2^8}$).

We now consider the finite field with 256 elements $\mathbb{F}_{2^8}$ (also noted $\mathbb{F}_{256}$) as the set of binary polynomials modulo $f = x^8 + x^4 + x^3 + x + 1$. (Note that we omit the (x) notation which is now superfluous since all polynomials are in x.)

Let $a = x^6 + x^4 + x^2 + x + 1 = 01010111$ and $b = x^7 + 1 = 10000001$, both elements of $\mathbb{F}_{256}$. Compute

(i) $a + b$,

(ii) $a \cdot b$, and

(iii) a^{-1}.

Exercise 1.4 (Correlation).

The security of a block cipher like AES depends crucially on a sufficient amount of nonlinearity. The following notion is an important measure of nonlinearity.

Given two functions $h, \ell \colon \mathbb{F}_{256} \to \mathbb{F}_2$ we define their *correlation*

$$\operatorname{corr}(h, \ell) = \sum_{a \in \mathbb{F}_{256}} (-1)^{h(a)+\ell(a)},$$

Thus we add 1 for every element where h and ℓ coincide and we subtract 1 for every element where they differ. The higher the value, the more h and ℓ coincide. In fact

$$\begin{aligned}\frac{1}{256}\operatorname{corr}(h, \ell) &= 2\operatorname{prob}(h(X) = \ell(X)) - 1\\ &= \operatorname{prob}(h(X) = \ell(X)) - \operatorname{prob}(h(X) \neq \ell(X)),\end{aligned}$$

if X is uniformly distributed in $\mathbb{F}_{256}$; the correlation of h and ℓ is thus a direct measure for the probability that h and ℓ coincide on a random input.

A field element $a \in \mathbb{F}_{256}$ can be represented in the form $a = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \mod x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_{256}$.

(i) A function $\ell \colon \mathbb{F}_{256} \to \mathbb{F}_2$ is *linear* if $\ell(a + b) = \ell(a) + \ell(b)$ for all $a, b \in \mathbb{F}_{256}$. Show that a linear function ℓ is always of the form $\ell(a) = \sum_i \ell_i a_i \in \mathbb{F}_2$ with suitable $\ell_i \in \mathbb{F}_2$.

(ii) Compute all possible values of corr(h, ℓ), if h and ℓ are linear. *Hint*: Without loss of generatility you can assume that h is the zero function.

(iii) Use your favourite programming language to compute the correlations corr$(\ell_i \circ h_j, \ell_k)$ of the following functions. Compute a little matrix for each h_j.

- $h_{-1}(a) := a^{-1}$ for $a \neq 0$ and $h_{-1}(0) = 0$,
- $h_1(a) := a$,
- $h_2(a) := a^2$,
- $h_3(a) := a^3$,
- $h_*(a) := (a_7 + a_6)x^7 + (a_3 + a_5)x^6 + (a_6 + a_5)x^5 + (a_2 + a_7 + a_4)x^4 + (a_5 + a_7 + a_4 + a_6)x^3 + (a_1 + a_5)x^2 + (a_7 + a_4 + a_6)x + a_6 + a_0 + a_4$.

- $\ell_0(a) := a_0$,
- $\ell_1(a) := a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7$,
- $\ell_2(a) := a_0 + a_4 + a_7$,
- $\ell_3(a) := a_5 + a_7 + 1$,
- $\ell_4(a) := a_5 + a_7$.

(iv) Draw conclusions from the results.