Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

7. Exercise sheet
Hand in solutions until Saturday, 14 December 2013, 23:59:59

Exercise 7.1 (The Advanced Encryption Standard running). (10 points)

In this exercise we put hands on the Advanced Encryption Standard (AES). There are three versions standardized, each with 128, 192 and 256 bit keys, respectively. We will play with AES-128, the version employing a 128 bit key.

(i) Find a library implementing the AES-128 in a programming language of your choice. Name the library and explain why you selected it. $\boxed{2}$

(ii) Now, using a randomly selected key (you might use the all zeroes key as well), run AES-128 for $i = 0 \ldots 27$ on 2^i blocks encoding the block number j in some suitable fashion. For example, the 128-bit block corresponding to $j = 1$ would be $\boxed{5}$

$$\underbrace{00\ldots00}_{\text{127 zeroes}}1.$$

Compute average runtime and deviation on each of the 2^i encryptions.

(iii) Interpret the results. $\boxed{3}$

Exercise 7.2 (Adding on elliptic curves). (5 points)

Assume you are given an elliptic curve $E\colon y^2 = x^3 + ax + b$ in Weierstraß form over a finite field $\mathbb{F}_q$ and two finite points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on it with $P \neq \pm Q$. Derive a formula for the point $P + Q$ by considering the line through P and Q. $\boxed{5}$

Exercise 7.3 (Count it!). (4+4 points)

Let $E\colon y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$ with characteristic neither 2 nor 3. Denote by $E(\mathbb{F}_q)$ the set of F_q-rational points on the curve E (i.e. those points with coordinates in $\mathbb{F}_q$) and write $\#E(\mathbb{F}_q)$ for the number of $\mathbb{F}_q$-rational points on the curve.

(i) Consider the (generalized) Legendre symbol $\boxed{2}$

$$\left(\frac{a}{\mathbb{F}_q}\right) := \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if there is } b \in \mathbb{F}_q \text{ with } b^2 = a, \\ -1 & \text{if there is no } b \in \mathbb{F}_q \text{ with } b^2 = a. \end{cases}$$

Prove that $\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+ax+b}{\mathbb{F}_q}\right)$.

$\boxed{2}$ (ii) Consider the curve $E\colon y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. Compute $\#E(\mathbb{F}_5)$ using the formula from (i).

$\boxed{+4}$ (iii) Consider the same situation over $\mathbb{F}_{5^2} = \mathbb{F}_5[x]/(x^2 + x + 1)$. Compute $\#E(\mathbb{F}_{5^2})$ using the formula from (i).

Exercise 7.4 (Associativity). (0+7 points)

$\boxed{+7}$ Show, using a computer algebra system of your choice, that the group law on elliptic curves in Weierstraß form $E\colon y^2 = x^3 + ax + b$ as defined in the lecture is associative. That is for any points P, Q, S on the curve, we have $(P + Q) + S = P + (Q + S)$.

Hint: Do not consider any special cases, i.e. assume that in all occurring additions we add finite points U, V with $U \neq \pm V$. To show the result you will have to use the curve equation repeatedly!