EXERCISES

Exercice 1 *Sort by difficulty the following computations:*

1. *factoring a 1024-bit RSA key;*
2. *computing discrete logs in* $(\mathbb{Z}/p\mathbb{Z})^*$ *when* p *is a* 1024 *bit prime and* $p-1 = 2p'$ *with* p' *prime;*
3. *computing discrete logs in* $\mathbb{F}^*_{2^{1024}}$*;*
4. *factoring* $2^{1039}-1$*;*
5. *computing discrete logs on an ordinary elliptic curve of cardinality* Q*, a* 256*-bit prime;*

Give arguments for each sign $<$ *in the sorted list that you obtained.*

Exercice 2 *Let* $N = \frac{7^{26}-2^{26}}{3}$.

1. *Show that* N *is an integer.*
2. *Can you write* N *as* $n_1 \times n_1$ *with* $2 \leq n_1, n_2 \leq N-1$ *?*

Exercice 3 *We propose a variant of RSA : Alice picks two random primes* p *and* q *of* 512 *bits each and computes* $N = pq$*, its public key. Its private key is* $d = p||q$*, the concatenation of* p *and* q*. Bob encypher messages of up to* 1000 *bits and we add* 24 *control bits before encryption: the sum of the bits, the sum of the bits of even indices, the sum of bits of index divisible by* 3*, etc., to obtain* m*, the plaintext to be transmitted. The encryption of* m *is*

$$c = m^3 + m + 1.$$

In order to decypher, Alice finds the the roots of $x^3+x+1-c$ *modulo* p *and* q*. Give your comments on this variant of RSA.*

You can discuss the validity and the complexity of encryption and decryption, the possible weaknesses of the system, the weak keys N*. Is it less safe to store* $p||q$ *rather than* $\varphi(N)$ *(as is the case for RSA)? What is the reason of adding the control bits?*

Exercice 4 *We want to implement the Index Calculus algorithm to compute discrete logarithms in* $F = \mathbb{F}_3[X]/\langle X^3 - x + 1\rangle$.

1. *If the smoothness bound is* 1*, what is the factor base ?*
2. *Use the relation* $x^3 \equiv x + 2 \pmod{x^3 - x + 1}$ *to write a linear equation among discrete logarithms of elements in the factor base.*
3. *Pinpointing consists in generating new relations using translations:* $x \mapsto x+1$*. What linear system do you obtain ?*
4. *Compute* $\log_{x+1} u$ *for all* u *in the factor base.*

Exercice 5 *In the Index calculus algorithm for* $(\mathbb{Z}/p\mathbb{Z})^*$ *a relation is an exponent* e *such that* $(g^e \bmod p) = \prod_{q \ prime} q^{e_q}$ *for some integers* e_q*. Show that the matrix which is associated to the relations system has at most* $\log_2 p$ *non-zero entries per row.*

Exercice 6 *Let A be a matrix of size $10M \times 10M$ and 100 nonzero-entries row. Each element is in the interval $[0, p-1]$ for some prime p of 160 bits. We want to solve the linear system $Ay = 0$.*

1. *What is (an approximation) of the RAM used to store the matrix ?*
2. *Explain how to compute xA^iy for $i = 0, 1, \ldots, 10M$. What is the approximative number of operations if one operation= one addition or multiplication of two 64 bit integers ?*
3. *We split the matrix in 4 and call $A_{0,0}$ and $A_{0,1}$ the two upper blocks of A and call $A_{1,0}$ and $A_{1,1}$ the two lower blocks. If y_0 and y_1 are the upper and the lower half of a column, how do you compute Ay on four cores ?*
4. *It turns out that the number of non-zero entries per row and per column decreases in a continuous way from top to botton and from left to right so that the $A_{0,0}$ is much more heavy than $A_{1,1}$.*
   (a) *Explain why we can reorder the rows of the matrix without storing any information.*
   (b) *We decide to reorder the columns of the matrix A and call A' the new matrix: let's say we only which the first and the third column. How do you obtain a solution of the system $Ay = 0$ if you are given a solution z of $A'z = 0$?*
   (c) *Give a simple way of reordering the columns and the rows so that the four cores work at the same speed.*