Summerschool crypt@b-it 2010

JOACHIM VON ZUR GATHEN, DANIEL LOEBENBERGER, MICHAEL NÜSKEN

1. Preparation sheet

Basics.

Exercise 1.1 (φ-asco). *Let $p, q \in \mathbb{N}$ be two different prime numbers. Let $N = p \cdot q$. Then $\varphi(N) = (p-1) \cdot (q-1)$. Compute — without factoring N — p and q, if $N = 168149075693$ and $\varphi(N) = 168148245408$ are given.* Hint: *Look at the quadratic equation $x^2 - (p+q)x + pq = 0$.*

Exercise 1.2 (Reductions). *Consider some problems:*

Problem (RSA). *Given a number N which is a product of two primes p and q (of approximately same size), a number e coprime to $\varphi(N) = (p-1)(q-1)$, and a number $y \in \mathbb{Z}_N^\times$. Compute x such that $y = x^e$ in $\mathbb{Z}_N^\times$.*

Problem (Factoring). *Given a number N which is a product of at least two distinct primes compute all prime factors of N.*

Problem (CSAT). *Given a boolean formula $\varphi(x_1, \ldots, x_n)$. Find $u_1, \ldots, u_n \in \{0,1\}$ such that $\varphi(u_1, \ldots, u_n) = 1$. [We consider 1 as true and 0 as false.]*

(i) Reduce the RSA problem to factoring, ie. write down a program for the RSA problem using a subroutine for factoring. Make sure that the runtime of your reduction (counting the subroutine as one time step) is polynomial in the input size.

(ii) Reduce factoring to CSAT in polynomial time.

Exercise 1.3 (Signatures). *Fix a multiplicatively written group G of your choice, an element $g \in G$ whose order ℓ has a large prime factor, and a cryptographic hash function $h\colon \{0,1\}^* \to \mathbb{Z}_\ell$. [Ie. h can be efficiently calculated but there is (hopefully) no polynomial time algorithm to find $m_1, m_2 \in \{0,1\}^*$ such that $m_1 \neq m_2$ and $h(m_1) = h(m_2)$.] Whoever wants to sign documents prepares a key pair (α, a) consisting of a private key $\alpha \in \mathbb{Z}_\ell$ and a public key $a = g^\alpha \in G$. The public key is distributed.*

An ElGamal signature *of a document $m \in \{0,1\}$ is a pair $(b, \gamma) \in G \times \mathbb{Z}_\ell$ such that*

$$a^{b^*} b^\gamma = g^{h(m)}.$$

(i) *Rewrite all the previous for an additively written group $\mathcal{G}$, an element $G \in \mathcal{G}$, private key $a \in \mathbb{Z}_\ell$, public key $A \in \mathcal{G}$.*

(ii) *Denote by $\langle g \rangle$ the subgroup of G generated by g, ie. $\langle g \rangle = \{g^\beta \mid \beta \in \mathbb{Z}\}$. Prove that the exponentiation map*

$$\begin{array}{rcl} \mathbb{Z}_\ell & \longrightarrow & \langle g \rangle\,, \\ \beta & \longmapsto & g^\beta, \end{array}$$

is a group isomorphism.

(iii) *Prove that the exponentiation map can be calculated efficiently (ie. in polynomial time).*

Contrasting this, computing the inverse of the exponentiation map is the discrete logarithm problem which is supposed to be difficult in many cases.

(iv) *Forging a signature means to generate a document m with a valid signature (b, γ) knowing the user's public key a but not her private key. Reduce forging a signature to solving the discrete logarithm problem in polynomial time.*

(v) *The signer produces a signature by first choosing $b = g^\beta$ with $\beta \in_R \mathbb{Z}_\ell^\times$. Explain how and that she can always generate a valid signature to an arbitrary document m.*

Lattice-based cryptanalysis.

Exercise 1.4 (Lattices). *Let $a_1, \ldots, a_m \in \mathbb{R}^n$ be linearly independent over $\mathbb{R}$. Then*

$$L = \sum_{1 \le i \le m} \mathbb{Z} a_i = \left\{ \sum_{1 \le i \le m} r_i a_i \colon r_1, \ldots, r_m \in \mathbb{Z} \right\}$$

is the lattice *spanned by $a_1, \ldots, a_m$. These vectors form a* basis *of L. We usually write the basis as a matrix A whose row-vectors are $a_1, \ldots, a_m$.*

Now let $m = 2$, $a_1 = (12, 2)$, $a_2 = (13, 4)$ and $L = \mathbb{Z}a_1 + \mathbb{Z}a_2$.

(i) *Sketch the set of lattice points together with the basis a_1, a_2.*

(ii) *Is the point $(1, 2)$ in the lattice? What about the point $(4, 5)$?*

(iii) *Are the two vectors $b_1 = (1, 2), b_2 = (9, -4)$ also a basis of L?*

Exercise 1.5 (Gram-Schmidt orthogonalization). *Denote for two vectors $u, v \in \mathbb{R}^n$ their scalar product as $\langle u, v\rangle := \sum_{1\le i\le n} u_i v_i$. Remember Gram-Schmidt orthogonalization from your course on linear algebra. There we constructed, given a basis $B \in \mathbb{R}^{m\times n}$ of the vectorspace $V := \mathrm{span}(B)$, an orthogonal basis B^* of the same space by defining $b_1^* := b_1$, $b_i^* := b_i - \sum_{j<i} \mu_{i,j} b_j^*$ with $\mu_{i,j} := \frac{\langle b_i, b_j^*\rangle}{\langle b_j^*, b_j^*\rangle}$.*

(i) Show that for $i_1 \neq i_2$ the vectors $b_{i_1}^*$ and $b_{i_2}^*$ are orthogonal.

(ii) Show that for $i < j$ the vectors b_i and b_j^* are orthogonal.

(iii) Consider the vector space $V = \mathrm{span}(B)$, spanned by the basis

$$B := \begin{bmatrix} 2 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{bmatrix}.$$

Compute an orthogonal basis of V.

(iv) Is your orthogonal basis of V also a basis of the lattice spanned by B? Justify your answer.

(v) Construct out of the Gram-Schmidt orthogonalization procedure a method which returns an orthonormal basis, i.e. an orthogonal basis B^*, where we have for all b_i^* that $\|b_i^*\| = 1$.

Exercise 1.6 (Two notes on the volume). *Let $A \in \mathbb{R}^{n\times n}$ a basis of the lattice L. In this case one defines the* volume *of the lattice as* $\mathrm{vol}(L) = \det(A)$.

(i) Show that this definition of the volume is independent of the choice of the basis. Hint: If $B \in \mathbb{R}^{n\times n}$ is another basis of L, express the vectors of this basis in terms of the basis A.

(ii) Let B^* be the orthogonalization of B. Prove that $\mathrm{vol}(L) = \prod_i \|b_i^*\|$. Hint: Use the fact that $B^* = BT$ for some upper triangular matrix T with $T_{i,i} = 1$ for all $i = 1 \dots m$.

Pairing-based cryptography.

Exercise 1.7 (Elliptic Curves). *We consider the curve given by the equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{R}$. Such a curve is given by the set of all pairs $(u, v) \in \mathbb{R}^2$ such that $v^2 = u^3 + au + b$. In particular if the curve is given by an equation of the above type (plus some additional technical conditions which we omit here), the curve is called an* elliptic curve.

(i) Sketch a graph of the elliptic curves $\mathcal{E} : y^2 = x^3 - 3x + b$ over the reals $\mathbb{R}$, for $b \in \{1, 2, 3\}$.

(ii) *Are the points* $P = (0,1)$, $Q = (-\frac{3}{2}, \sqrt{\frac{17}{8}})$, $T = (-2,0)$ *on the elliptic curve* $y^2 = x^3 - 3x + 1$*?*

(iii) *Draw the line through* P *and* Q*.*

(iv) *Compute the third intersection point* R *of this line and the curve* $\mathcal{E}$*.*

Actually, whenever two distinct points P, Q *on the curve are joined by a line this line will meet the curve in exactly one further point* R*. Requiring* $P + Q + R = \mathcal{O}$ *will (almost) turn the curve into a group. ***MAGIC****

For that to work out nicely the curve must not have 'corners' (as in case $a = 0$, $b = 0$*) or 'double-points' (as in case* $a = -3$, $b = 2$*): A curve* $\mathcal{E}$ *is called* smooth *if all of its points have a unique tangent line. In our case, this means that the curve equation* $y^2 = x^3 + ax + b$*, its* x*-derivative* $0 = 3x^2 + a$ *and its* y*-derivative* $2y = 0$ *have no common solution.*

(v) *Show that the curve given by*

$$f = y^2 - x^3 - ax - b$$

is smooth if and only if

$$4a^3 + 27b^2 \neq 0.$$

Exercise 1.8 (Read!). *Read the papers given on our preparation-page*

`http://cosec.bit.uni-bonn.de/students/events/cryptabit2010/10us-cryptabit-prep/`.

Note that you may need to create a password for your cosec web account at

`http://cosec.bit.uni-bonn.de/myaccount/`

for easier access to the papers.