# Solution

## Cryptography – Homework 6

Discussed on **Wednesday**, 14th January, 2015.

*For questions regarding the exercises, please send an email to schlund@model.in.tum.de or just drop by at room 03.11.055*

(∗) Starred exercises are optional and are usually not discussed during the tutorial (nevertheless they are fun—hopefully).

### Exercise 6.1 The RSA Problem and Factoring

We currently do not know if the RSA Problem is equivalent to the factoring problem. We only know that factoring the RSA modulus can be reduced to a number of problems: Suppose Eve is given $(N, e)$ show that she can efficiently factor $N = pq$ in each of the following cases:

(a) she can efficiently compute $\varphi(N)$ (Hint: Show $q^2 - q(N + 1 - \varphi(N))) + N = 0$).

(b) she can efficiently compute an $x \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$.

**Solution:**

(a) We have $q - (N + 1 - (p - 1)(q - 1)) + p = 0$. Multiplying by $q(\neq 0)$ yields the identity in the hint. Given this identity we see that once we know $\varphi(N)$ we can obtain $q$ (and thus $p$) by solving a quadratic equation (over the reals!) which can be done in polynomial time.

(b) If $x \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$ then $\gcd(x, N) > 1$ and thus $\gcd(x, N) = p$ or $\gcd(x, N) = q$. $\gcd(x, N)$ can of course be computed efficiently using Euclid's Algorithm.

### Exercise 6.2 Computing Discrete Logarithms

Let $p$ be prime. Assume there is a generator $g \in \mathbb{Z}_p^*$ such that computing the discrete logarithm in $\mathbb{Z}_p^*$ with respect to $g$ can be done efficiently. Show that then the discrete logarithm with respect to any other generator $g'$ of $\mathbb{Z}_p^*$ can also be computed efficiently.

**Solution:** Let $g \neq g'$ and $y \in \mathbb{Z}_p^*$. We show: Computing $x$ with $(g')^x = y$ in $\mathbb{Z}_p^*$ can be reduced to computing discrete logarithms using $g$ as base.

- Since $g$ is a generator of $\mathbb{Z}_p^*$, we know that there exists a $k \in \{1, \dots, p - 1\}$ such that $g^k = g'$ in $\mathbb{Z}_p^*$. Now we can restate the problem as $(g')^x = y \Leftrightarrow g^{kx} = y$.
- Recall now that for every $s \in \mathbb{N}$, since $p$ is prime,

$$g^s = g^{s \bmod (p-1)} \text{ holds in } \mathbb{Z}_p^*.$$

The idea is to exponentiate $g^{kx}$ by a suitable $l$ to "get rid" of the $k$ in the computation. For this we show that $\gcd(k, p-1) = 1$. Assume that $\gcd(k, p - 1) = d \geq 1$. Then there are $\alpha, \beta \in \mathbb{N}$ such that $k = d \cdot \alpha$ and $(p - 1) = d \cdot \beta$. Hence $\beta \leq p - 1$. Now we compute in $\mathbb{Z}_p^*$:

$$(g')^\beta = \left(g^k\right)^\beta = g^{d\alpha\beta} = g^{\alpha(p-1)} = 1,$$

since $(p-1)$ is the order of $\mathbb{Z}_p^*$. Hence $g'$ can generate at most $\beta$ elements in $\mathbb{Z}_p^*$: $p-1 = o_{g'} \leq \beta \leq p-1$. Hence $\beta = p-1$ and $d = 1$. With this we can compute $l \in \mathbb{Z}_{p-1}^*$ such that $l \cdot k = 1$ in $\mathbb{Z}_{p-1}^*$ (using e.g. the extended Euclidean algorithm).

- Now we calculate in $\mathbb{Z}_p^*$:

$$\begin{aligned} & g^{kx} = y \\ \Leftrightarrow\ & g^{kxl} = y^l && (\text{ Exponentiate with } l) \\ \Leftrightarrow\ & g^{klx \bmod (p-1)} = y^l && (\phi(p) = p-1) \\ \Leftrightarrow\ & g^x = y^l && (k \cdot l \equiv 1 \bmod (p-1)) \end{aligned}$$

In summary, the following steps are needed for computing $x$ such that $g^x = y$:

1. Compute $k \in \{1, \ldots, p-1\}$ such that $g^k = g'$ in $\mathbb{Z}_p^*$.
2. Compute $l \in \{1, \ldots, p-2\}$ such that $k \cdot l = 1$ in $\mathbb{Z}_{p-1}^*$.
3. Compute $x \in \{1, \ldots, p-1\}$ such that $g^x = y^l$ in $\mathbb{Z}_p^*$.

## Exercise 6.3 Hardcore!

(a) Let $f$ be a OWF. Show that $h(x) = \bigoplus_{i=0}^{n-1} x_i$ is in general *not* a hardcore predicate for $f$. (Hint: define a new OWF $g$ which leaks the value of $h(x)$)

(b) Let $\mathcal{F}$ be a (collection of) bijective functions from $\{0,1\}^n$ to $\{0,1\}^n$. Show: if $\mathcal{F}$ has a hardcore-predicate then $\mathcal{F}$ is a OWP.

**Solution:**

(a) $g(x) := (f(x), h(x))$ is an OWF: if we had an algorithm $\mathcal{A}$ for obtaining (with a non-negligible prob.) a preimage of $g(x)$ we could use it to find a preimage (with a non-negligible prob.) of $f(x)$ simply by feeding $\mathcal{A}$ with $(f(x), 0)$ and $(f(x), 1)$ and checking if any of its two outputs is a preimage of $g(x)$. However it is clear that $h(x)$ is not a hardcore predicate **for** $g$ (given $g(x) = (a, b)$ the second component $b$ is the value of $h(x)$).

(b) Suppose $\mathcal{F}$ were no OWP then there would exist an algorithm $\mathcal{A}$ that finds a preimage of a given $f(x)$ with non-neg. prob. Thus given $f(x)$ we would feed it to $\mathcal{A}$, obtain an $x'$ (with $f(x') = f(x)$ with non-neg. prob.). As $f$ is bijective we have $x' = x$ with the same probability and thus $h(x) = h(x')$ which we can compute given $x'$.

## Exercise 6.4 From the exam in 2012

(a) Let $\langle \mathbb{G}, \cdot, 1 \rangle$ be a finite cyclic group with generator $g$. Denote by $q := |\mathbb{G}|$ the order of $\mathbb{G}$. Assume $q = d \cdot m$ is a composite and let $d$ be a non-trivial factor of $q$. Let $y \in \mathbb{G}$.

Show: If $k \in \mathbb{N}$ satisfies $g^k = y$ in $\mathbb{G}$, then $(k \bmod d)$ is the unique solution of the following problem:

$$\text{Determine } x \in \mathbb{Z}_d \text{ such that } (g^m)^x = y^m \text{ in } \mathbb{G}.$$

(b) Given are the prime 89 and the generator 3 of $\langle \mathbb{Z}_{89}^*, \cdot, 1 \rangle$. Your task is to determine $k \in \mathbb{Z}$ such that $3^k \equiv 86 \pmod{89}$. Proceed as follows:

i) Using the preceding exercise, first determine $k$ modulo 11.

ii) Someone tells you that $k \equiv 5 \pmod 8$. Determine $k$.

**Solution:**

(a) We have to show two things: (1) $(k \bmod d)$ is a solution and (2) it is unique For (1): that if $g^k = y$ in $G$ then $(g^k)^m = y^m$ (and of course $(g^k)^m = g^{km} = (g^m)^k$). $g^m$ has order $d$ and hence $y^m = (g^m)^k = (g^m)^{(k \bmod d)}$.

For (2): Let $x \in \mathbb{Z}_d$ satisfy the equation, i.e. $(g^m)^x = y^m$ (we have to show that $x = (k \bmod d)$). Then we have $(g^m)^x = (g^m)^{(k \bmod d)}$ and thus $(g^m)^{x-(k \bmod d)} = 1$, i.e. $x \equiv_d (k \bmod d)$ and since $x$ and $(k \bmod d)$ are both less than $d$ we obtain $x = (k \bmod d)$.

(b) i) Since $|\mathbb{Z}_{89}^*| = 88 = 8 \cdot 11$, by the preceding exercise we need to find $x$ such that

$$(3^8)^x = 86^8 = (-3)^8 = 3^8 \pmod{89}$$

However, this is trivial: $x = 1$ and hence, $k \equiv_{11} 1$.

ii) By the CRT we have that $\mathbb{Z}_{88}$ is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_{11}$ and the inverse isomorphism $h^{-1} : \mathbb{Z}_8 \times \mathbb{Z}_{11} \to \mathbb{Z}_{88}$ is given by $h^{-1}(x, y) = 3 \cdot 11 \cdot x - 4 \cdot 8 \cdot y \pmod{88}$. Hence $k = h^{-1}(5, 1) = 133 = 45 \pmod{88}$. Thus, $3^{45} = 86 \pmod{88}$.

**Exercise 6.5*** **Mersenne primes**

The largest known prime numbers are Mersenne primes $M$ (as of today the largest is $2^{57,885,161}-1$ which was found in 2013 by the GIMPS). Mersenne primes are primes of the form $2^p-1$ for some prime $p$.

(a) Find the first four Mersenne primes

(b) Factor $2^9-1$.

(c) There is a simple reason why the exponent in the definition must be a prime: For composite exponents $n$ the number $2^n-1$ is a composite — Prove this statement!

**Solution:**

(a) The first four Mersenne primes are: $3, 7, 31, 127$

(b) $2^9-1$ is *not* prime (because 9 is not prime): $2^9-1 = 7 \cdot 73 = (2^3-1)\cdot(1+2^3+2^6)$

(c) Suppose $n$ is composite, i.e. $n = a \cdot b$ with some $a, b > 1 \in \mathbb{N}$. From the finite geometric sum

$$\sum_{i=0}^{b-1}(2^a)^i = \frac{(2^a)^b-1}{2^a-1}$$

we obtain:

$$2^n-1 = (2^a)^b-1 = \left(\sum_{i=0}^{b-1}(2^a)^i\right)\cdot(2^a-1)$$

which gives us an explicit factorization of $2^n-1$ (both factors are $>1$).