Cryptography (SS2006) Prof. Michael Backes

Exercise Sheet 5

Out: May 31, 2006 Saarland University

Problem 1: Discrete Logarithm is Easy in $\mathbb{Z}^*_{2^n+1}$

Let $p = 2^n + 1$ be a prime for $n \in \mathbb{N}$, g a generator of $\mathbb{Z}^*_p$, and $h \in \mathbb{Z}^*_p$. Show that computing the discrete logarithm $\mathsf{DLog}_g(h)$ is easy in $\mathbb{Z}^*_p$, i.e., give an algorithm that efficiently computes $\mathsf{DLog}_g(h)$.
Hints:

- Write the logarithm as $\mathsf{DLog}_g(h) =: x = \sum_{i=0}^{n-1} x_i 2^i$.
- Use the fact that $g^y = g^z \bmod 2^n + 1$ iff $y = z \bmod 2^n$.
- Show that $x_0 = 1$ iff $h^{2^{n-1}} = g^{2^{n-1}} \bmod p$.
- Show that $x_1 = 1$ iff $h^{2^{n-2}} = g^{2^{n-1}} \cdot g^{x_0 \cdot 2^{n-2}} \bmod p$.
- Find a recursive algorithm to compute x_i for $i = 2, \ldots, n-1$.

Problem 2: Random Self-reducibility of CDH

Let p be a prime and g be a generator of $\mathbb{Z}^*_p$. Suppose that there exists an algorithm A for computing g^{xy} in time T whenever $(g^x, g^y) \in S_1 \times S_2$, where $S_1, S_2 \subseteq \mathbb{Z}^*_p$ are arbitrary sets with $|S_1| = |S_2| = \epsilon \cdot |\mathbb{Z}^*_p|$. Construct an algorithm B for computing g^{xy} for all $(g^x, g^y) \in \mathbb{Z}^*_p \times \mathbb{Z}^*_p$ in expected time T/ϵ^2.

Problem 3: Cyclic Groups

Let p, q primes with $p = 2q + 1$, and let $g \in \mathbb{Z}^*_p$.

(a) Prove that $< g >= \mathbb{Z}^*_p \Leftrightarrow (g^q \neq 1 \ \wedge \ g^2 \neq 1)$

(b) Let furthermore $i \in \mathbb{N}$. Prove $\big(< g >= \mathbb{Z}^*_p \wedge 2 \not| \, i \wedge q \not| \, i\big) \Rightarrow < g^i >= \mathbb{Z}^*_p$.

Problem 4: Some Computations

(a) Compute 30^{-1} in $\mathbb{Z}^*_{73}$

(b) Compute $\sqrt[2]{11}$ in $\mathbb{Z}^*_{19}$

(c) Compute $\sqrt[2]{5}$ in $\mathbb{Z}^*_{11}$

Compute the following values using Repeated Squaring:

(d) 3^{42} in $\mathbb{Z}^*_{101}$

(e) 7^{23} in $\mathbb{Z}^*_{107}$