Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

11. Exercise sheet
Hand in solutions until Saturday, 02 July 2011, 23:59h.

To estimate the average effort you put into solving the following exercises, please add after each exercise the amount of time you spent for it.

Exercise 11.1 (DLP with CRT and Pohlig-Hellman). (11 points)

Let G be the multiplicative group $\mathbb{Z}_{73}^{\times}$. Consider the two elements $g = 5$ and $x = 6$.

(i) Verify that g is a generator of G. 2

(ii) Compute $a = \mathrm{d}\ell\mathrm{og}_g\, x$ as follows: Determine a modulo 8 from $x^9 = (g^9)^a$. (The order of g^9 is 8.) Determine a modulo 9 from $x^8 = (g^8)^a$. (The order of g^8 is 9.) Combine these two congruences to compute a modulo 72. 3

Now let $G = \mathbb{Z}_{163}^{\times}$, $g = 7$ and $x = 20$.

(iii) Prove that $\mathrm{ord}(g) = 162$. 2

(iv) Compute $a = \mathrm{d}\ell\mathrm{og}_g\, x$ as follows: Determine a modulo 2 from $x^{81} = (g^{81})^a$ as in (ii). To determine a modulo 81 we modify our approach. 4

Let $\tilde{a} = a \text{ rem } 81$, $\tilde{x} = x^2$ and $\tilde{g} = g^2$, so that $\tilde{a}$ is determined by $\tilde{x} = \tilde{g}^{\tilde{a}}$. The idea is now, to use the *p-adic extension* $\tilde{a} = \sum_{i=0}^{3} a_i 3^i$ with $a_i \in \{0, 1, 2\}$. Deduce the value of a_0 from $\tilde{x}^{27} = (\tilde{g}^{27})^{\tilde{a}} = (\tilde{g}^{27})^{a_0}$. (Give a justification for the last equality.) After that consider $\tilde{x}^9 = (\tilde{g}^9)^{\tilde{a}} = (\tilde{g}^9)^{a_0}(\tilde{g}^{27})^{a_1}$ to deduce a_1. (Again, justify the last equality.) Continue to compute $\tilde{a}$ and combine it with the result for a modulo 2 to obtain a.

Exercise 11.2. (3 points)

You and your bank want to agree on a common key via the `Diffie-Hellman protocol` in a multiplicative group $\mathbb{Z}_p^{\times}$. You know that in order to do so, a *large* prime number p has to be chosen and a generator for the multiplicative group $\mathbb{Z}_p^{\times}$ has to be determined. These may be tedious tasks. 3

As part of their Christmas campaign, the hardware company PIERPONTPRIMES-UNLIMITED advertises their exceptionally fast and cheap hardware for computations in specific multiplicative groups $\mathbb{Z}_p^{\times}$. Your bank has received a tempting offer, where p is the following 1024-bit prime number:

```
10731372821463388140252972760123405140333921422866431822 8\
5946106897867885100815144444489959819534285998417753835 1\
95113972071934508791317051724287708017495853963774546810 7\
81650040365117150438772174380687075627001093191509346011 3\
17823940014927377049254581980549545296496847611743859688 2\
0366678237029638036520 97
```

Of course, a long list of generators is included, so they would also spare themselves the work of searching for one of those.

Now, your bank turns to you: Since those two pieces of information (the chosen group and the chosen generator) are public anyways, there seems to be no reason to reject this offer.

Reply to this and justify your answer. (You may assume that the hardware really does the computations as claimed and nothing else.)

Exercise 11.3 (Change of generators). (8 points)

Let G be a finite cyclic group of order d. Let g be a generator of G. Let us see, what we can find about possible other generators of G and the consequences for DL_G.

3 (i) Given a generator g, only certain powers g^i qualify as generators of G. Find out which and prove your criterion.

2 (ii) Given two generators g and g', the respective discrete logarithms for an arbitrary element $x \in G$ are linked by the fundamental identity

$$\mathrm{d}\ell\mathrm{og}_{g'} x = \mathrm{d}\ell\mathrm{og}_g x \, \mathrm{d}\ell\mathrm{og}_{g'} g.$$

Prove it.

3 (iii) Given two generators g and g' of G, prove the polynomial-time equivalence

$$\mathrm{DL}_g = \mathrm{DL}_{g'}.$$