Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, KONSTANTIN ZIEGLER

6. Assignment: Chinese distribution and Pohlig-Hellman for discrete logarithms

(Due: Wednesday, 10 December 2008, 13^{40}, b-it bitmax)

Exercise 6.1 (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 $a = \operatorname{dlog}_g x$ 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 $\operatorname{ord}(g) = 162$. [2]

(iv) Compute $a = \operatorname{dlog}_g x$ 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 $\tilde{a} = a$ 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 *3-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 6.2. (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:

```
1073137282146338814025297276012340514033392142286643182 28\
5946106897867885100815144444489959819534285998417753833 51\
9511397207193450879131705172428770801749585396377454681 07\
8165004036511715043877217438068707562700109319150934601 13\
1782394001492737704925458198054954529649684761174385968 82\
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.)

(Hint: To spare you the nuisance of copying 309 decimal digits, there is a text-file containing p on the course-webpage.)