Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

3. Exercise sheet
Hand in solutions until Saturday, 26 April 2014, 23:59:59

Exercise 3.1 (Pollard rho for discrete logarithms). (5 points)

Consider the group $G = \mathbb{Z}_{25}^{\times}$ generated by the element $g = 2 \in G$. Compute the discrete logarithm of $x = 17 \in G$ to the base g using the Pollard rho method. Use the partition $S_0 = \{1, 2, 3, 4, 6, 7, 8\}$, $S_1 = \{9, 11, 12, 13, 14, 16, 17\}$, and $S_2 = \{18, 19, 21, 22, 23, 24\}$ of G, with $7, 7$, and 6 elements, respectively. Hint: If the computation returns "failure" persist in computing the discrete logarithm by the method presented in the lecture. [5]

Exercise 3.2 (Chinese remaindering for Discrete Logarithms). (8 points)

(i) Let G be a cyclic group of size d and g be a generator of G. Let q be a divisor of d and consider the map $\pi\colon G \to G$, with $\pi(x) = x^{d/q}$. Prove that $\pi(G) = \{y \in G\colon y^q = 1\}$. [3]

(ii) Let $G = \mathbb{Z}_p^{\times}$ with $p = 2 \cdot 3 \cdot 5 \cdot 7 + 1$, $g = 2$, $x = 10$. Compute the discrete logarithm of x in base g using the Chinese remainder theorem. [5]

Exercise 3.3 (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 $a = \mathrm{dlog}_g\, x$ 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 $\mathrm{ord}(g) = 162$. [2]

(iv) Compute $a = \mathrm{dlog}_g\, x$ 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 *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.