# Introduction to Modern Cryptography, Exercise # 9


University of Amsterdam, Master of Logic
Lecturer: Christian Schaffner
TA: Joachim Schipper


8 November 2011
(to be handed in by Tuesday, 15 November 2011, 9:00)

1. **Euler Phi Function:** Exercise 7.4 in [KL]

2. **Calculations:**

   (a) Compute (by hand) the final two (decimal) digits of $3^{1000}$ (Exercise 7.5 in [KL]). **Hint:** The answer is $[3^{1000} \mod 100]$.

   (b) Compute $[101^{4'800'000'023} \mod 35]$ by hand (Exercise 7.6 in [KL]).

   (c) Find a $x \in \mathbb{Z}_{9999}$ that fulfills the following system of congruences:

   $$13x \equiv 4 \mod 99$$
   $$15x \equiv 56 \mod 101\,.$$

   **Hint:** First use the Extended Euclidean Algorithm to invert $13 \mod 99$ and $15 \mod 101$ in order to obtain a system of congruences where the coefficients of $x$ are 1, then apply the Chinese Remainder theorem. You may want to use a calculator, there are *many* (simple) calculations in this exercise.

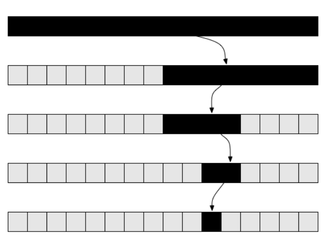
3. **Efficient Test for Perfect Powers:** Exercise 7.11 in [KL]. Give an explicit algorithm for (b), and show (informally) that it is polytime. **Hint:** (a) $\|N\|$ is the number of bits required to represent $N$.

4. **Index Calculus "Light":** Let $p = 227$. $p$ is prime, so $\alpha = 2$ is a generator of $\mathbb{Z}_p^*$.

   (a) Compute $\alpha^{32}$, $\alpha^{40}$, $\alpha^{59}$ and $\alpha^{156}$ modulo $p$, and factor them over the integers. The prime factors should all be in the "factor base" $\{2, 3, 5, 7, 11\}$.

   (b) Using the fact that $\log 2 = 1$, compute $\log 3$, $\log 5$, $\log 7$ and $\log 11$ from the factorizations obtained above (all logarithms are discrete logarithms in $\mathbb{Z}_p^*$ with respect to the base $\alpha$).

   (c) Now suppose we wish to compute $\log 173$. Multiply 173 by $2^{177} \mod p$ (this algorithm requires a random power of 2, and fails for some "unlucky" values. We selected a random "lucky" value for you.) Factor the result over the factor base, and proceed to compute $\log 173$ using the previously computed logarithms of the numbers in the factor base.



Binary Search
Image credit: `http://www.codeido.com`.