Introduction to Modern Cryptography
Exercise Sheet #5

University of Amsterdam, Master of Logic, 2012
Lecturer: Christian Schaffner
TA: Maria Velema

27 November 2012
(to be handed in by Wednesday, 5 December 2012, 11:00)

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 α^{32}, α^{40}, α^{59} and α^{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 α).

   (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.

5. **Hybrid Encryption**

   (a) **Computational Indistinguishability:** Show that computational indistinguishability of probability ensembles (as defined in Definition 6.34 of [KL]) is transitive. Show that if both $X \stackrel{c}{\equiv} Y$ and $Y \stackrel{c}{\equiv} Z$ hold, we also have $X \stackrel{c}{\equiv} Z$.

(b) **Reduction:** Using the notation from the lecture, show that $(pk, \mathsf{Enc}_{pk}(k), \widetilde{\mathsf{Enc}}_k(m_0)) \stackrel{c}{\equiv} (pk, \mathsf{Enc}_{pk}(0^n), \widetilde{\mathsf{Enc}}_k(m_0))$. Consider a distinguisher $\mathcal{D}$ which distinguishes the above ensembles with probability $\varepsilon_{\mathcal{D}}(n)$, i.e.

$$\varepsilon_{\mathcal{D}}(n) = \left| \Pr[\mathcal{D}(pk, \mathsf{Enc}_{pk}(k), \widetilde{\mathsf{Enc}}_k(m_0)) = 1] - \Pr[\mathcal{D}(pk, \mathsf{Enc}_{pk}(0^n), \widetilde{\mathsf{Enc}}_k(m_0)) = 1] \right| .$$

In order to show that $\varepsilon_{\mathcal{D}}(n) \leq \mathsf{negl}(n)$, construct a CPA-attacker $\mathcal{A}$ on Π which uses $\mathcal{D}$ as a subroutine. **Hint**: Look at the proof of Theorem 10.13 in [KL]. Note that the solution must be in your own words.

6. **Impossibility Of Public-Key Encryption that is**

   (a) **perfectly-secure:** Exercise 10.1 in [KL]

   (b) **deterministic and secure:** Exercise 10.2 in [KL]

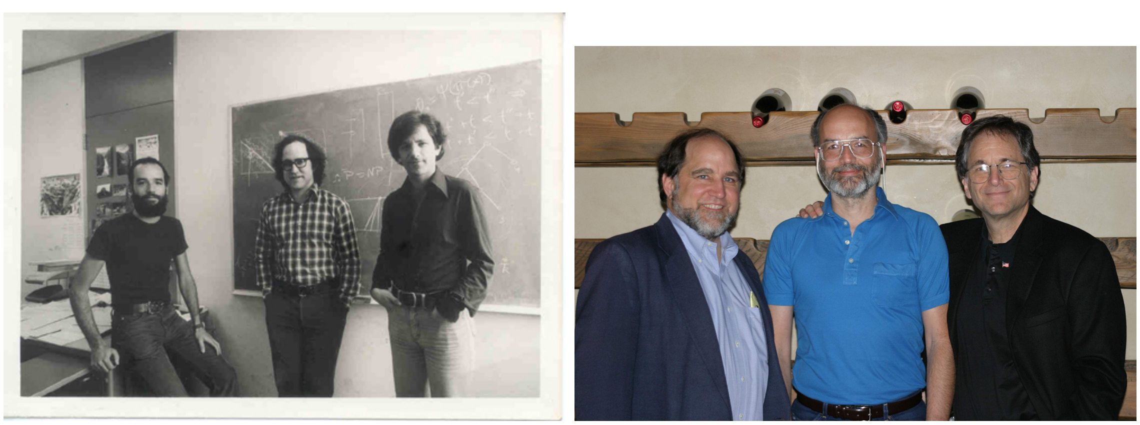
7. **Factoring RSA Moduli:** Let $N = pq$ be a RSA-modulus and let $(N, e, d) \leftarrow \mathsf{GenRSA}$. In this exercise, you show that for the special case of $e = 3$, computing d is equivalent to factoring N. Show the following:

   (a) The ability of efficiently factoring N allows to compute d efficiently. This shows one implication.

   (b) Given $\phi(N)$ and N, show how to compute p and q. **Hint:** Derive a quadratic equation (over the integers) in the unknown p.

   (c) Assume we know $e = 3$ and $d \in \{1, 2, \ldots, \phi(N) - 1\}$ such that $ed \equiv 1 \mod \phi(N)$. Show how to efficiently compute p and q. **Hint:** Obtain a small list of possibilities for $\phi(N)$ and use (b).

   (d) Given $e = 3$, $d = 29'531$ and $N = 44'719$, factor N using the method above.



Adi Shamir, Ron Rivest, and Len Adleman as MIT-students and in 2003

Image credit: `http://www.ams.org/samplings/feature-column/fcarc-internet`, `http://www.usc.edu/dept/molecular-science/RSA-2003.htm`.