Introduction to Modern Cryptography, Exercise # 10

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

15 November 2011
(to be handed in by Tuesday, 22 November 2011, 9:00)

1. **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.

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

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

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

3. **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.

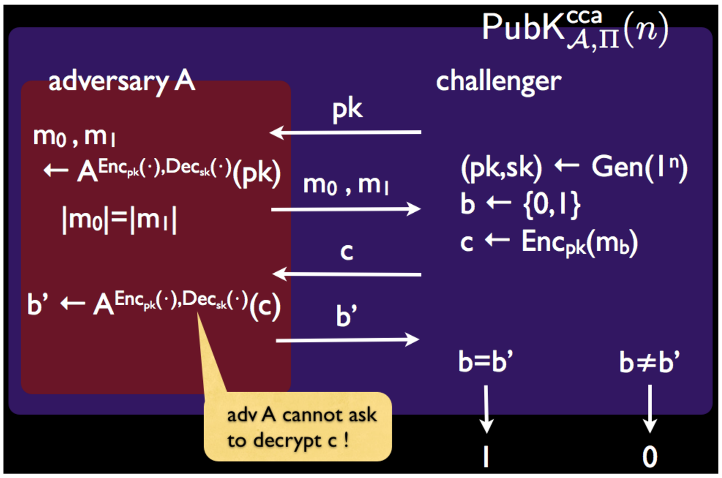
   (a) The ability of efficiently factoring N allows to compute d efficiently. This shows one implication.

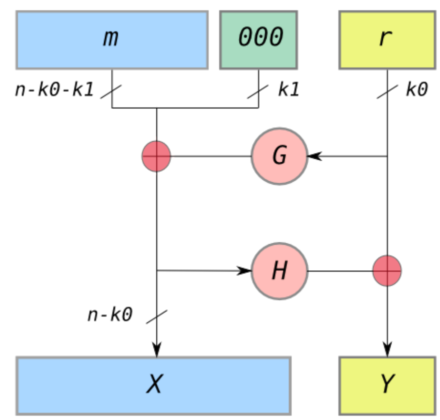
   (b) Given $\phi(N)$ and N, show how to compute p and q. **Hint:** Derive a quadratic equation (over the integers) in the unknown p.

   (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).

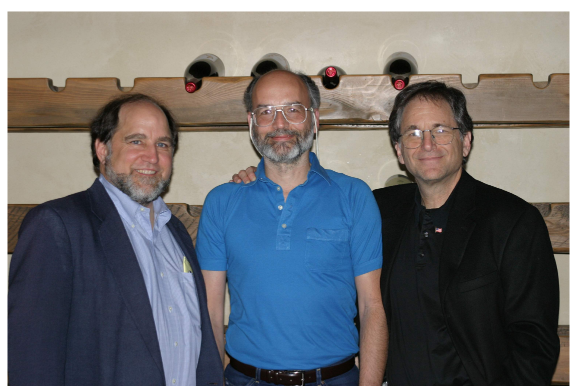
   (d) Given $e = 3$, $d = 29'531$ and $N = 44'719$, factor N using the method above.

4. **RSA-Padding and CCA-Security:** Exercise 10.14 in [KL]. **Hint:** Use messages m_0, m_1 whose ciphertexts you can transform into different valid ciphertexts if the most significant bit of the random part r of the padding is 0.





left: The $\mathsf{PubK}^{\mathsf{cca}}_{\mathcal{A},\Pi}(n)$ experiment, right: Optimal Asymmetric Encryption Padding (OAEP)
Image credit: `wikimedia.org`.



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`.