Introduction to Modern Cryptography
Exercise Sheet #1

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

30 October 2012
(to be handed in by Wednesday, 7 November 2012, 9:00)

1. **Exhaustive Search Over Key Space** Assume an adversary attacks an encryption scheme by exhaustive search over the key space $\mathcal{K}$. For simplicity, we assume that checking one key takes exactly one thousand clock cycles. Consider the two cases when the adversary is

   (a) an average Master of Logic student,

   (b) an American three-letter agency (FBI, CIA, NSA, ...).

   For both cases, make and *clearly state* reasonable assumptions about their computing power. How large does the key space $|\mathcal{K}|$ need to be so that a complete exhaustive search takes at least 10 years to complete.

   Note that three-letter agencies will not use PCs but more dedicated hardware for this purpose. `http://www.copacobana.org/`, for instance, can search through 2^{64} keys in 12.8 days and costs €9000 (all figures are about the 2007 model.)

2. Exercise 1.2 in the Katz & Lindell book [KL]

3. Exercise 1.5 in [KL]

4. Exercise 1.6 in [KL]

5. Exercise 2.3 from [KL].

6. Exercise 2.4 from [KL]. **Hint:** Use part (a) in part (c).

7. Exercises 2.7 and 2.8 from [KL]. You do *not* need to prove Exercise 2.6. You can just use the result.

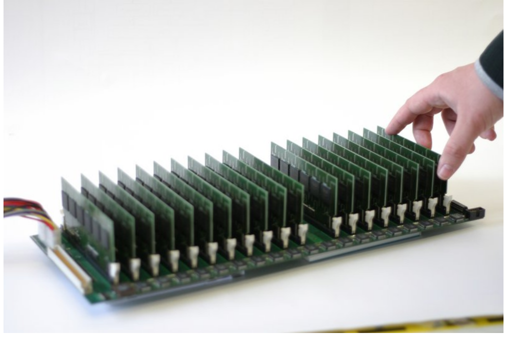

Figure 1: The COPACOBANA. Image credit: `http://www.copacobana.org`