Introduction to Modern Cryptography, Exercise # 1

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

6 September 2011
(to be handed in by Tuesday, 13 September 2011, 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 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]

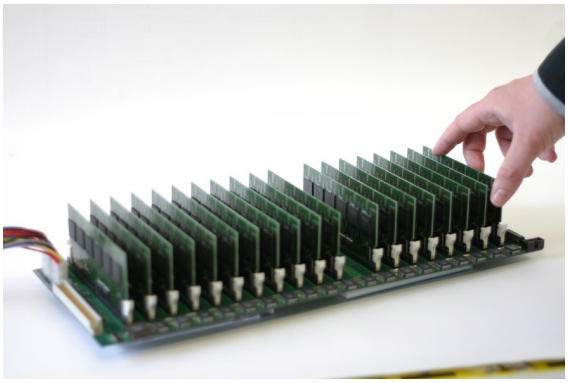

Figure 1: The COPACOBANA. Image credit: `www.copacobana.org`.