Introduction to Modern Cryptography
Exercise Sheet #1

University of Amsterdam, Master of Logic, 2014
Lecturer: Christian Schaffner
TA: Malvin Gattinger

Monday, 1 September 2014
(to be handed in by Monday, 8 September 2014, 11:00)

Homework

1. **Email** Please send an email to Malvin (malvin@w4eg.de) and Chris (c.schaffner@uva.nl) stating your name, the program and year you are following (e.g. 2nd year Master of Logic), and (at least) one sentence about your motivation to follow this course. `5 p.`

2. **Probabilities** Let the probability that a certain cryptographic protocol is *secure* and *efficient* be 10%. The probability that it is *not secure* if it is *effficient* is 80%. What is the probability that `10 p.`

   (a) the protocol is *secure* if it is *efficient*?

   (b) the protocol is *efficient*?

3. **Asymptotic notation** `25 p.`

   Definition 1 *Let $f(n), g(n)$ be functions from non-negative integers to non-negative reals. Then:*

   - $f(n) = O(g(n))$ *means that there exist a positive integer n' and a positive real constant $c > 0$ such that for all $n > n'$ it holds that $f(n) \leq c \cdot g(n)$.*
   - $f(n) = \Omega(g(n))$ *means that there exist a positive integer n' and a positive real constant $c > 0$ such that for all $n > n'$ it holds that $f(n) \geq c \cdot g(n)$.*
   - $f(n) = \Theta(g(n))$ *means that $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.*
   - $f(n) = o(g(n))$ *means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.*
   - $f(n) = \omega(g(n))$ *means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty$.*

   Show the following:

   (a) $f(n) = o(g(n))$ implies $f(n) = O(g(n))$.

   (b) For any constant $c > 1$, it holds that $\log_c n = \Theta(\log_2 n)$.

   (c) For $f(n) = e^{\sqrt{n}}$, it holds that $f(n) = O(2^n)$.

(d) Let ε and c be arbitrary constants such that $0 < \varepsilon < 1 < c$. Order the following terms in increasing order of their asymptotic growth rates.

$$n^n \quad \exp(\sqrt{\log n \log\log n}) \quad 1 \quad \log\log n \quad c^{c^n} \quad n^c \quad n^\varepsilon \quad n^{\log n} \quad \log n \quad c^n$$

Hint: In some cases, it might help to express two terms you want to compare in the form $e^{\cdots}$ and then compare their exponents.

4. **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 `10 p.`

   (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.) See `http://en.wikipedia.org/wiki/Brute-force_attack` for more details.

5. Exercise 1.2 in the Katz & Lindell book [KL] `10 p.`

6. Exercise 1.5 in [KL] `15 p.`

7. Exercise 1.6 in [KL] `15 p.`

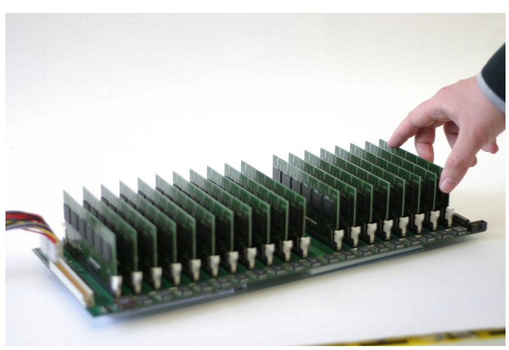

Figure 1: The COPACOBANA. Image credit: `http://www.copacobana.org`