Introduction to Modern Cryptography, Quiz

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

8 September 2011 (slightly improved version)
(to be handed in anonymously, but immediately)

All the theory in this quiz is copied from the appendix of the [KL]-book.

1. **Asymptotic notation**

   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.

2. **Probability theory** Let E_1 and E_2 be probability events. Then, $E_1 \wedge E_2$ denotes their conjunction, i.e. $E_1 \wedge E_2$ is the event that *both* E_1 and E_2 occur. The *conditional probability of E_1 given E_2*, denoted $\Pr[E_1|E_2]$ is defined as

   $$\Pr[E_1|E_2] := \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$$

   as long as $\Pr[E_2] \neq 0$. Prove Bayes' theorem.

Theorem 1 (Bayes' theorem) *If* $\Pr[E_2] \neq 0$ *then*

$$\Pr[E_1|E_2] = \frac{\Pr[E_1] \cdot \Pr[E_2|E_1]}{\Pr[E_2]} .$$

For an event E, the event $\bar{E}$ is the event that E does not occur, hence $\Pr[\bar{E}] = 1 - \Pr[E]$. The events E_1 and E_2 are said to be *independent* if $\Pr[E_1 \wedge E_2] = \Pr[E_1] \cdot \Pr[E_2]$. The disjunction event $E_1 \vee E_2$ is the event that either E_1 or E_2 (or both) occur. The *union bound* states that for arbitrary events E_1, E_2, we have

$$\Pr[E_1 \vee E_2] \leq \Pr[E_1] + \Pr[E_2] .$$

Prove the following inequality for real numbers $p_1, p_2, \ldots, p_n \in [0, 1]$:

$$(1 - p_1)(1 - p_2) \cdots (1 - p_n) \geq 1 - p_1 - p_2 - \ldots - p_n$$

by considering *independent* events E_i with probabilities $p_i = \Pr[E_i]$ and using the union bound.

The "Birthday" Problem If we choose q elements $y_1, \ldots, y_q$ uniformly at random from a set of size N (with replacements), we are interested in the probability that there exist distinct i, j with $y_i = y_j$. We refer to the stated event as a *collision*, and denote the probability of this event by $\mathsf{coll}(q, N)$. In Appendix A.4 of the [KL]-book, it is shown that if $q < \sqrt{N}$, the probability of a collision is $\Theta(q^2/N)$; alternatively, for $q = \Theta(\sqrt{N})$, the probability of a collision is constant.[1]

If we select 2^{64} elements uniformly at random from some set, and we want that any two of the chosen elements coincide with probability at most 2^{-40}, how large must the set be?

3. **Basic Number Theory** For $a, b \in \mathbb{Z}$, we say that a *divides* b, written $a \mid b$, if there exists an integer $c \in \mathbb{Z}$ such that $ac = b$. The *greatest common divisor* $\gcd(a, b)$ of two integers a, b is the largest integer c such that $c \mid a$ and $c \mid b$. Using the extended Euclidean algorithm, one can find integers X, Y such that $Xa + Yb = \gcd(a, b)$. Furthermore, $\gcd(a, b)$ is the smallest positive integer that can be expressed in this way.

   Let $a, b, N \in \mathbb{Z}$ with $N > 1$. By "division with remainder", there exist unique q, r such that $a = qN + r$ with $0 \leq r < N$. We call this remainder r the *reduction of a modulo N* and denote it by $[a \mod N]$.

   We say that *a and b are congruent modulo N*, written $a = b \mod N$, if $[a \mod N] = [b \mod N]$.

   If for a given integer a there exists an integer a^{-1} such that $a \cdot a^{-1} = 1 \mod N$, we say that a^{-1} is a (multiplicative) *inverse* of a modulo N and call a *invertible.*

   (a) List all eight common divisors of 12 and 18. What is $\gcd(12, 18)$?

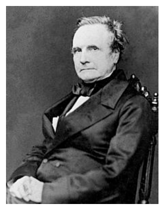
[1] This bound is sometimes referred to as "birthday paradox", because the collision probability $\mathsf{coll}(q, 365)$ gets large for pretty small values of q. For example, the probability that among 23 people two people have the same birthday is more than 50%. Among 57 people, the chance is 99%.

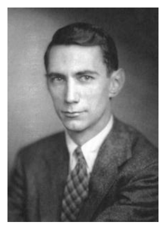
(b) Compute (by hand) $[1094029 \cdot 1320101 \mod 100]$.

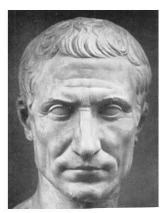
(c) $ab = cb \mod N$ does *not* necessarily imply $a = c \mod N$. Find a non-trivial counterexample a, b, c with $N = 12$ where none of a, b, c equals 0 mod N.

(d) Let a, N be integers with $N > 1$. Show that a is invertible modulo N if and only if $\gcd(a, N) = 1$.

4. Name the following people. The possible names in alphabetical order (and ROT-3 encrypted) are Fkduohv Edeedjh, Mxolxv Fdhvdu, Rghg Jroguhlfk, Vkdil Jrogzdvvhu, Mrq Ndwc, Dxjxvwh Nhufnkriiv, Bhkxgd Olqghoo, Vloylr Plfdol, Mrdfklp Vfklsshu, Fodxgh Vkdqqrq, Eodlvh gh Yljhqhuh.

(a)  (b)  (c)  (d) 

(e)  (f)  (g)  (h) 

(i)  (j)  (k) 

Hint: Their real names are Charles Babbage, Julius Caesar, Oded Goldreich, Shafi Goldwasser, Jonathan Katz, Auguste Kerckhoffs, Yehuda Lindell, Silvio Micali, Joachim Schipper, Claude Shannon, Blaise de Vigenère.