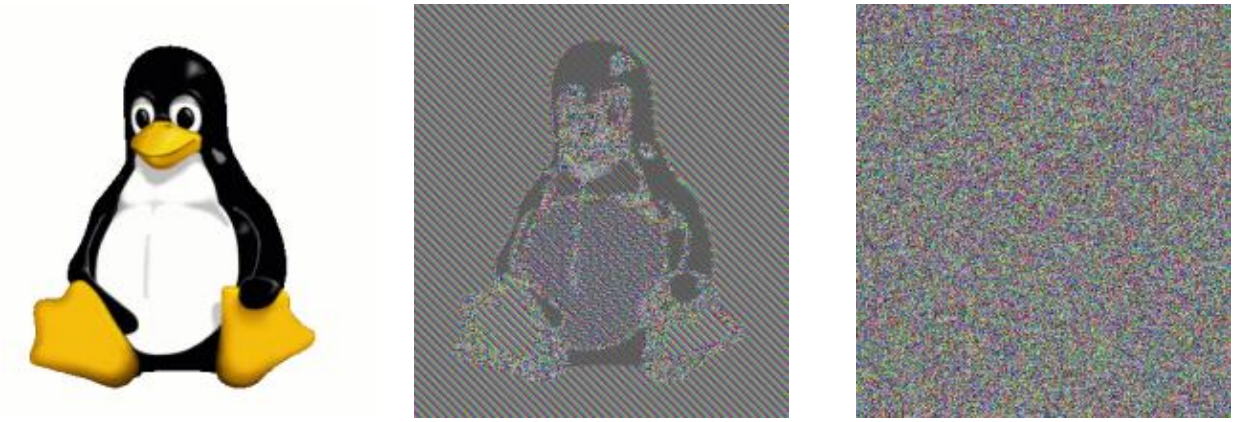
Introduction to Modern Cryptography
Exercise Sheet #2

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

6 November 2012
(to be handed in by Wednesday, 14 November 2012, 9:00)

1. Exercise 3.1 from [KL].
2. Exercise 3.3 from [KL].
3. Exercise 3.5 from [KL].
4. Exercise 3.6 from [KL]. Prove your answers. **Clarification:** in (a), the input to G, $s0^{|s|}$, is the concatenation of the string s with the all-zero string of the same bit-length as s.
5. Exercise 3.9 from [KL].
6. Exercise 3.15 from [KL]. **Hint for (a)** Construct a pseudorandom generator G such that $G(k) = G(k+1)$ for every even k.
7. Consider a variant of CBC-mode encryption, where the sender uses $IV = 1$ the first time, $IV = 2$ the next time, $IV = 3$ the third time, etc. Show that this variant is *not* CPA-secure. This problem lies at the heart of the "BEAST SSL attack" which has been in the news last year. Read more about it on the web, e.g. `http://goo.gl/jKxIi`.
8. Exercise 3.21 from [KL].



left: original picture, middle: encrypted using ECB mode, right: secure encryption mode
Image credit: `Larry Ewing, The GIMP, wikimedia.org` .