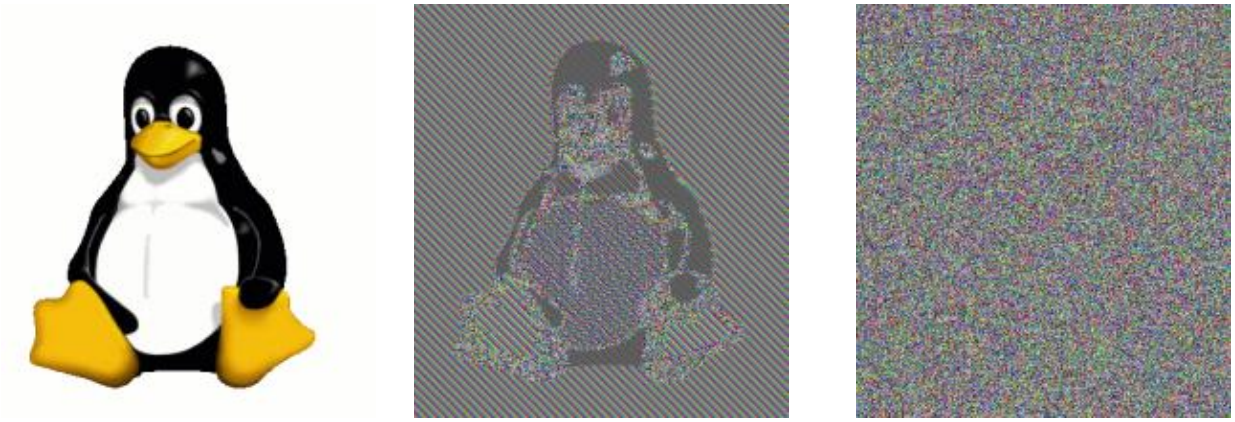
Introduction to Modern Cryptography, Exercise # 4

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

27 September 2011
(to be handed in by Tuesday, 4 October 2011, 9:00)

1. Exercise 3.9 from [KL].
2. Exercise 3.15 from [KL]. **Hint for (a)** Construct a pseudorandom generator G such that $G(k) = G(k+1)$ for every even k.
3. 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. Search the web for "BEAST SSL attack" to read about recent consequences of this problem.
4. 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` .