# Introduction to Modern Cryptography
# Exercise Sheet #3

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

Monday, 15 September 2014
(to be handed in by Monday, 22 September 2014, 11:00)

## Homework

1. Exercise 3.9 from [KL]. "Present a construction of a variable output-length pseudorandom generator from any pseudorandom function. Prove that your construction satisfies Definition 3.17 (variable output-length pseudorandom generator". `10 p.`

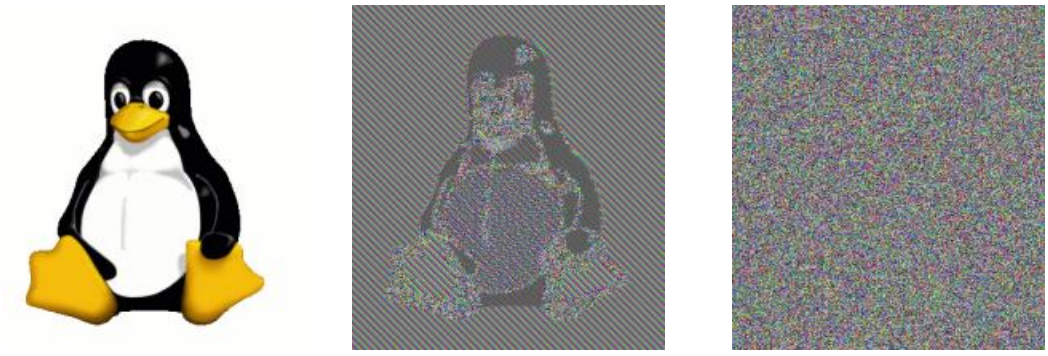
2. Exercise 3.15 from [KL]. "Let F be a pseudorandom function, and G a pseudorandom generator with ..." **Clarification of (a):** In this exercise, $k+1$ for $k \in \{0,1\}^n$ should be interpreted as flipping the last bit of $k$, i.e. $k+1 := k \oplus 0^{n-1}1$. **Hint for (a):** Let $G' : \{0,1\}^{n-1} \to \{0,1\}^{\ell(n)}$ be a PRG. Construct from $G'$ a $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ such that $G(k) = G(k \oplus 0^{n-1}1)$ for every $k \in \{0,1\}^n$ and show that $G$ is a PRG. Use that PRG $G$ to show that the proposed scheme is *not* secure. `20 p.`

3. Exercise 3.21 from [KL]. "Let $\Pi_1$ and $\Pi_2$ be two encryption schemes for which it is known that at least one is CPA-secure ...". Use the hint! `10 p.`

4. Show that one has to be very careful with modifications of CBC-MAC, small modifications can be disastrous. Exercises 4.9 and 4.8 of [KL]. `15 p.`

5. Exercise 3.22 from [KL]. "Show that the CBC, OFB, and counter modes of encryption do not yield CCA-secure encryption schemes (regardless of F)." `10 p.`

6. Insecurity of Encrypt-and-Authenticate: Exercise 4.19 of [KL]. "Show that if any message authentication code having unique tags is used in the encrypt-and-authenticate approach, the resulting combination is not CPA-secure." `10 p.`



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

**more on the back side**

7. **Different security goals should always use independent keys!** We derive an example what can go wrong if the same key is used in the Encrypt-then-Authenticate approach (which yields CCA-security if independent keys are used!). 15 p.

Let $F$ be a strong pseudorandom permutation according to Definition 3.28 in [KL]. Let the key $k \leftarrow \{0,1\}^n$ be picked uniformly at random by $\mathsf{Gen}$. Define $\mathsf{Enc}_k(m) = F_k(m\|r)$ for $m \in \{0,1\}^{n/2}$ and a random $r \leftarrow \{0,1\}^{n/2}$, and define $\mathsf{Mac}_k(c) = F_k^{-1}(c)$.

(a) Define the corresponding decryption function $\mathsf{Dec}_k(\cdot)$ and prove that this encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CPA-secure.

(b) Prove that the authentication code is a secure MAC.

(c) Conclude that the combination of the two schemes in the Encrypt-then-Authenticate approach *using the same key $k$* is completely insecure.