Cryptography, winter term 16/17: Assignment 2

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due November 16, 2016

Exercise 2.1 (Messing up the one-time pad) Consider the following modification of the *one-time pad*:

- $\mathcal{K} = \mathcal{M} = \{0,1\}^\ell, \mathcal{C} = \{0,1\}^{\ell+1}$
- GEN generates a uniform key
- ENC outputs $c := (m \oplus k)||\text{Parity}(k)$ (on input (k, m))
- DEC outputs $m := (c_1 \dots c_\ell) \oplus k$ (on input $(c = c_1, \dots c_\ell c_{\ell+1}, k)$)

where $\oplus$ is the bitwise exclusive-or, $||$ is string concatenation and $\text{Parity}(k)$ is defined as the number of 1s in k modulo 2.
We give an example: Let $\ell = 6$, $m = 101010$ and assume GEN did output the key $k = 110010$. As the number of 1s in k is odd, it holds that $\text{Parity}(k) = 1$. Therefore

$$\text{ENC}_k(m) = (m \oplus k)||\text{Parity}(k) = 011000||1 = 0110001$$

and

$$\text{DEC}_k(c) = (c_1c_2c_3c_4c_5c_6) \oplus k = 011000 \oplus 110010 = 101010$$

Prove that this modification of the one-time pad is not perfectly secret.
Hint: A common way to show that a scheme is not perfectly secret is to construct an adversary $\mathcal{A}$ and to show that $\mathcal{A}$ wins the *adversarial indistinguishability experiment* with probability $> \frac{1}{2}$.

Exercise 2.2 (Negligible functions) Recall the definition of a *negligible* function (Definition 3.4).

(a) Let c be a constant. Which of the following two functions is negligible? Prove your answer.
   (i) $f(n) := \binom{n}{c}^{-1}$
   (ii) $g(n) := (\log n)^{-\log n}$

(b) Prove Proposition 3.6.

Exercise 2.3 (Perfect secrecy) Recall Lemma 2.4. One direction was proven in the lecture. In this exercise it is your task to prove the other direction, i.e., show that *perfect secrecy* of $(\mathrm{GEN}, \mathrm{ENC}, \mathrm{DEC})$ implies

$$\Pr\left[\mathrm{ENC}_k(m) = c\right] = \Pr\left[\mathrm{ENC}_k(m') = c\right] \tag{1}$$

for all $m, m' \in \mathcal{M}, c \in \mathcal{C}$.

Exercise 2.4 (Perfect indistinguishability) Recall Lemma 2.6:

An encryption scheme Π *is perfectly secret if and only if it is perfectly indistinguishable.*

Prove *one direction of your choice.*
Hint: It may be advisable to use the equivalent definition of perfect secrecy as stated in Lemma 2.4.
Bonus: Prove the other direction as well.