Cornelius Brand, Marc Roth

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 $> \frac{1}{2}$.

Solution 2.1 (Messing up the one-time pad) We construct an adversary $\mathcal{A}$ that will always win: $\mathcal{A}$ sends messages $m_1 = 0^\ell$ and $m_2 = 0^{\ell-1}1$. After $\mathcal{A}$ recieves the challenge text $c = c_1 \dots c_\ell c_{\ell+1}$, it checks whether $\text{Parity}(c_1 \dots c_\ell \oplus m_1) = c_{\ell+1}$. If this is the case it outputs 1 otherwise it outputs 0.
We show that $\mathcal{A}$ is always right. If $b = 1$ then $c = (m_1 \oplus k)||\text{Parity}(k)$ and therefore $\text{Parity}(c_1 \dots c_\ell \oplus m_1) = \text{Parity}(m_1 \oplus k \oplus m_1) = \text{Parity}(k) = c_{\ell+1}$. It follows that $\mathcal{A}$ outputs 1 which is right.
If $b = 0$ then $c = (m_2 \oplus k)||\text{Parity}(k) = (m_1 \oplus 0^{\ell-1}1 \oplus k)||\text{Parity}(k)$ and therefore $\text{Parity}(c_1 \dots c_\ell \oplus m_1) = \text{Parity}(m_1 \oplus 0^{\ell-1}1 \oplus k \oplus m_1) = \text{Parity}(0^{\ell-1}1 \oplus k) \neq \text{Parity}(k) = c_{\ell+1}$. It follows that $\mathcal{A}$ outputs 0 which is right. Therefore

$$\Pr\left[\text{PrivK}^{\text{eav}}_{\mathcal{A},\Pi} = 1\right] = 1 > \frac{1}{2}$$

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.

Solution 2.2 (Negligible functions)

(a)

  (i) Not negligible: It holds that $\binom{n}{c} \leq n^c$ and therefore

$$\frac{1}{\binom{n}{c}} \geq \frac{1}{n^c}$$

  (ii) Negligible: Fix a constant c. It holds that

$$g(n) = (\log n)^{-\log n} = \frac{1}{n^{\log \log n}} < \frac{1}{n^c}$$

  for all n such that $\log \log n > c$.

(b) Let p be an arbitrary but fixed polynomial.

  (i) As p is a polynomial, $p'(x) := 2p(x)$ is also a polynomial. As negl_1 and negl_2 are negligible, there are N_1 and N_2 such that $\forall n \geq N_1 : \text{negl}_1(n) < \frac{1}{p'(n)}$ and $\forall n \geq N_2 : \text{negl}_2(n) < \frac{1}{p'(n)}$. Therefore

$$\forall n \geq \max\{N_1, N_2\} : \text{negl}_1(n) + \text{negl}_2(n) < \frac{1}{p(n)}$$

  (ii) We have to show that for a *fixed* polynomial q, it holds that there is an N such that forall $n \geq N$ we have

$$q(n) \cdot \text{negl}_1(n) < \frac{1}{p(n)}$$

  As q is a polynomial, $q \cdot p$ is also and as negl_1 is negligible we have that there exists an N such that

$$\forall n > N : \text{negl}_1(n) < \frac{1}{q(n) \cdot p(n)}$$

  Therefore

$$\forall n > N : q(n) \cdot \text{negl}_1(n) < q(n) \cdot \frac{1}{q(n) \cdot p(n)} = \frac{1}{p(n)}$$

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

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

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

Solution 2.3 (Perfect secrecy) Let m_1, m_2 and c be arbitrary but fixed and consider the following probability distribution over the message space $\mathcal{M}$:

$$\Pr[M = m] = \begin{cases} \frac{1}{2} & \text{if } m = m_1 \text{ or } m = m_2 \\ 0 & \text{otherwise} \end{cases}$$

Furthermore, let

$$P := \Pr[\mathrm{ENC}_k(m_1) = c] + \Pr[\mathrm{ENC}_k(m_2) = c]$$

If $P = 0$ we are done. Otherwise we have

$$\begin{aligned}
\Pr[\mathrm{ENC}_k(m_1) = c] &= P \cdot \frac{\Pr[\mathrm{ENC}_k(m_1) = c]}{P} \\
&= P \cdot \frac{\Pr[\mathrm{ENC}_k(m_1) = c] \cdot \frac{1}{2}}{\frac{1}{2} \cdot (\Pr[\mathrm{ENC}_k(m_1) = c] + \Pr[\mathrm{ENC}_k(m_2) = c])} \\
&= P \cdot \frac{\Pr[\mathrm{ENC}_k(m_1) = c] \cdot \Pr[M = m_1]}{\sum_{m \in \mathcal{M}} \Pr[\mathrm{ENC}_k(m) = c] \cdot \Pr[M = m]} \\
&= P \cdot \frac{\Pr[\mathrm{ENC}_k(M) = c | M = m_1] \cdot \Pr[M = m_1]}{\sum_{m \in \mathcal{M}} \Pr[\mathrm{ENC}_k(M) = c | M = m] \cdot \Pr[M = m]} \\
&= P \cdot \frac{\Pr[C = c | M = m_1] \cdot \Pr[M = m_1]}{\sum_{m \in \mathcal{M}} \Pr[C = c | M = m] \cdot \Pr[M = m]} \\
&= P \cdot \frac{\Pr[C = c | M = m_1] \cdot \Pr[M = m_1]}{\Pr[C = c]} \\
&= P \cdot \Pr[M = m_1 | C = c] = P \cdot \Pr[M = m_1] = \frac{P}{2}
\end{aligned}$$

Similary, with the same computation we get $\Pr[\mathrm{ENC}_k(m_2) = c] = \frac{P}{2}$ and therefore

$$\Pr[\mathrm{ENC}_k(m_1) = c] = \Pr[\mathrm{ENC}_k(m_2) = c]$$

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.

Solution 2.4 (Perfect indistinguishability) First we show that perfect secrecy implies perfect indistinguishability. Therefore let $\mathcal{A}$ be an arbitrary but fixed adversary. Consider an execution of the adversarial indistinguishability experiment. Let B be the bit that was chosen uniformly at random, $Chal$ be the ciphertext (the challenge) $\mathcal{A}$ recieved and B' the output of $\mathcal{A}$. We claim that

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1\right] = \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0 | B = 0\right]$$

which can be proven as follows:

$$\begin{aligned}
&\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1\right] \\
&= \Pr\left[B' = 1 | Chal = \mathrm{ENC}_k(m_1)\right] \\
&= \sum_{c \in \mathcal{C}} \Pr\left[B' = 1 | Chal = \mathrm{ENC}_k(m_1), \mathrm{ENC}_k(m_1) = c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_1) = c\right] \\
&= \sum_{c \in \mathcal{C}} \Pr\left[B' = 1 | Chal = c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_1) = c\right] \\
&= \sum_{c \in \mathcal{C}} \Pr\left[B' = 1 | Chal = c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_0) = c\right] \\
&= \sum_{c \in \mathcal{C}} \Pr\left[B' = 1 | Chal = \mathrm{ENC}_k(m_0), \mathrm{ENC}_k(m_0) = c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_0) = c\right] \\
&= \Pr\left[B' = 1 | Chal = \mathrm{ENC}_k(m_0)\right] \\
&= \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0 | B = 0\right]
\end{aligned}$$

where the fourth equation follows from perfect secrecy. Similary we can prove that

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 0\right] = \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0 | B = 1\right]$$

It follows that

$$\begin{aligned}
&\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\right] \\
&= \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1\right] \cdot \Pr\left[B = 1\right] + \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 0\right] \cdot \Pr\left[B = 0\right] \\
&= \frac{1}{2} \cdot \left(\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1\right] + \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 0\right]\right) \\
&= \frac{1}{2} \cdot \left(\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0 | B = 0\right] + \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0 | B = 1\right]\right) \\
&= \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0 | B = 0\right] \cdot \Pr\left[B = 0\right] + \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0 | B = 1\right] \cdot \Pr\left[B = 1\right] \\
&= \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0\right]
\end{aligned}$$

and therefore

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\right] = \frac{1}{2}$$

Now we show the that perfect indistinguishability implies perfect secrecy. Actually we show the contraposition, i.e., we assume that the encryption scheme is not perfect. In this case there are messages m_0, m_1 and a ciphertext and an $\epsilon > 0$ such that

$$\Pr\left[\mathrm{ENC}_k(m_1) = c\right] = \Pr\left[\mathrm{ENC}_k(m_0) = c\right] + \epsilon \tag{2}$$

We construct an adversary $\mathcal{A}$ as follows: $\mathcal{A}$ outputs m_1 and m_0 in the first step and as soon as it recieves a challenge c' it checks whether $c' = c$. If this is the case then $\mathcal{A}$ outputs 1 and otherwise it outputs a bit at random. The intuition behind the following computation can easily be seen by drawing the tree for the different cases of the experiment. Let B, and B' as before. It holds that

$$\begin{aligned}
&\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1\right] \\
&= (\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1, \mathrm{ENC}_k(m_1) = c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_1) = c\right] \\
&+ \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1, \mathrm{ENC}_k(m_1) \neq c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_1) \neq c\right]) \\
&= (1 \cdot \Pr\left[\mathrm{ENC}_k(m_1) = c\right] + \frac{1}{2} \cdot \Pr\left[\mathrm{ENC}_k(m_1) \neq c\right]) \\
&= \Pr\left[\mathrm{ENC}_k(m_1) = c\right] + \frac{1}{2} \cdot \Pr\left[\mathrm{ENC}_k(m_1) \neq c\right]
\end{aligned}$$

And furthermore we have

$$\begin{aligned}
&\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 0\right] \\
&= (\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 0, \mathrm{ENC}_k(m_0) = c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_0) = c\right] \\
&+ \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 0, \mathrm{ENC}_k(m_0) \neq c\right] \cdot \Pr\left[\mathrm{ENC}_k(m_0) \neq c\right]) \\
&= (0 \cdot \Pr\left[\mathrm{ENC}_k(m_0) = c\right] + \frac{1}{2} \cdot \Pr\left[\mathrm{ENC}_k(m_0) \neq c\right]) \\
&= \frac{1}{2} \cdot \Pr\left[\mathrm{ENC}_k(m_0) \neq c\right]
\end{aligned}$$

Putting these two together we get that

$$\begin{aligned}
&\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\right] \\
&= \frac{1}{2} \cdot \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 1\right] + \frac{1}{2} \cdot \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1 | B = 0\right] \\
&= \frac{1}{2} \Pr\left[\mathrm{ENC}_k(m_1) = c\right] + \frac{1}{4} \cdot \Pr\left[\mathrm{ENC}_k(m_1) \neq c\right] + \frac{1}{4} \cdot \Pr\left[\mathrm{ENC}_k(m_0) \neq c\right]
\end{aligned}$$

A similar computation yields

$$\begin{aligned}
&\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0\right] \\
&= \frac{1}{2} \Pr\left[\mathrm{ENC}_k(m_0) = c\right] + \frac{1}{4} \cdot \Pr\left[\mathrm{ENC}_k(m_0) \neq c\right] + \frac{1}{4} \cdot \Pr\left[\mathrm{ENC}_k(m_1) \neq c\right]
\end{aligned}$$

Using Equation 2 we conclude

$$\begin{aligned}
&\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\right] - \Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 0\right] \\
&= \frac{1}{2} \left(\frac{1}{2} \Pr\left[\mathrm{ENC}_k(m_1) = c\right] - \frac{1}{2} \Pr\left[\mathrm{ENC}_k(m_0) = c\right] \right) \\
&= \frac{\epsilon}{2} > 0
\end{aligned}$$

and therefore

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1\right] > \frac{1}{2}$$