3. Exercise sheet
Hand in solutions until Friday, 18 November 2016, 12:00 (noon)

Exercise 3.1 (OW-POA). (10 points)

One-wayness game $G_{\text{OW-POA}}$.
1. Prepare a key $k \leftarrow \text{KeyGen}(1^\kappa)$ in $K$.
2. Choose a plaintext $m \leftarrow M$ uniformly random.
3. Prepare a one-time oracle $O_{\text{Test}}$ that when called with no input the oracle returns $c \leftarrow \text{Enc}_k(m)$.
4. Call the attacker $\mathcal{A}$ with input $1^\kappa$ and the oracle $O_{\text{Test}}$. Await a guess $m' \in M$.
5. If $m = m'$ then ACCEPT else REJECT.

(i) Determine the success probability of the guessing attacker $\tilde{\mathcal{A}}$ that merely picks $m' \leftarrow M$ uniformly random.

(ii) Prove that every indistinguishable encryption scheme is also one-way secure, i.e. each probabilistic polynomial-time attacker has at most a negligible advantage in winning the game $G_{\text{OW-POA}}$.

Exercise 3.2 (Negligible or significant?). (4 points)

Decide which of the following functions are negligible or significant.

<table>
<thead>
<tr>
<th>$f$</th>
<th>$\frac{1}{\sqrt{\log_2 n}}$</th>
<th>$2 - \sin n \log_2 n$</th>
<th>$n^3 2^{-n}$</th>
<th>$\log_2^2 n / n^4$</th>
<th>$2 - n^2$</th>
<th>$2^{-\frac{1}{n^2}}$</th>
<th>$2^{-\frac{\log_2 n}{\log_2 \log_2 n}}$</th>
<th>$2^{-\frac{\log_2 n}{\sin n}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>negligible?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>significant?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exercise 3.3 (Visual cryptography). (0+12 points)

For visual cryptography we use slides to transport ciphertext and key. The overlay shall reveal the plainimage.

How does that work? For each pixel of the plainimage pick a pixel as a key consisting of $2 \times 2$ subpixels exactly two of which are white and two are black.

![Key pixel example]

The ciphertext consists of the same $2 \times 2$ pixel for a white plainimage pixel and the inverted pixel for a black one. To decrypt simply overlay ciphertext and key.

(i) Describe the full scheme in our language. Hint: Tell us exactly what the keyspace $K$, the plaintext space $M$ and the ciphertext space $C$ are. Then formulate what exactly KeyGen, Enc and Dec do.

Justify that your description is correct. Hint: Fit your construction to the above intuitive description and prove $\text{Dec}_k(\text{Enc}_k(m)) = m$.

(ii) Prove that the scheme is perfectly secret.