Cryptography, winter 2016/17

MICHAEL NÜSKEN, JAKOB NUSSBAUMER

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 $\mathcal{K}$.
2. Choose a plaintext $m \xleftarrow{\$} \mathcal{M}$ uniformly random.
3. Prepare a *one-time* oracle $\mathcal{O}_{\text{Test}}$ that when called with no input the oracle returns $c \leftarrow \text{Enc}_k(m)$.
4. Call the attacker $\mathcal{A}$ with input 1^κ and the oracle $\mathcal{O}_{\text{Test}}$. Await a guess $m' \in \mathcal{M}$.
5. If $m = m'$ then ACCEPT else REJECT .

(i) Determine the success probability of the guessing attacker $\widetilde{\mathcal{A}}$ that merely picks $m' \xleftarrow{\$} \mathcal{M}$ uniformly random. $\boxed{4}$

(ii) Prove that every indistinguishable encryption scheme is also one-way secure, ie. each probabilistic polynomial-time attacker has at most a negligible advantage in winning the game $G^{\text{OW-POA}}$. $\boxed{6}$

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

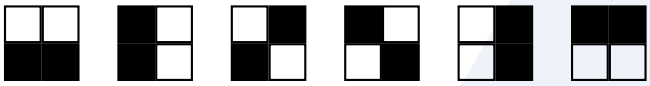
Decide which of the following functions are negligible or significant. $\boxed{4}$

f	$\frac{1}{\sqrt{\log_2 n}}$	$2^{-\sin n \cdot \log_2 n}$	$n^3 2^{-n}$	$\frac{\log_2 n}{n^4}$	2^{-n^2}	$2^{-\frac{1}{n}}$	$2^{-\frac{\log_2 n}{\log_2 \log_2 n}}$	$2^{-\frac{\log_2 n}{\sin n}}$
negligible?								
significant?								

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 2×2 subpixels exactly two of which are white and two are black.



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

+6 (i) Describe the full scheme in our language. *Hint:* Tell us exactly what the keyspace $\mathcal{K}$, the plaintext space $\mathcal{M}$ and the ciphertext space $\mathcal{C}$ 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 $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$.

+6 (ii) Prove that the scheme is perfectly secret.