Cryptography, winter 2015/16

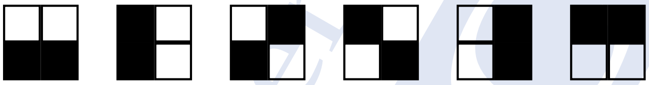
MICHAEL NÜSKEN, SIMON SCHNEIDER

3. Exercise sheet
Hand in solutions until Saturday, 21 November 2015, 12:00

Exercise 3.1 (Visual cryptography). (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.

(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. $\boxed{6}$

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

(ii) Prove that the scheme is perfectly secret. $\boxed{6}$

Exercise 3.2. (6 points)

Consider the following definition of perfect secrecy for the encryption of *two* messages. An encryption scheme $(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ over a message space $\mathcal{M}$ is *perfectly secret for two messages* if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$ and all $c, c' \in \mathcal{C}$ with $\mathrm{prob}\,(C = c \wedge C' = c') > 0$: $\boxed{6}$

$$\mathrm{prob}\,(M = m \wedge M' = m' \,|\, C = c \wedge C' = c') = \mathrm{prob}\,(M = m \wedge M' = m')$$

Here, M and M' are sampled from the same distribution over $\mathcal{M}$ and $C = \mathrm{Enc}_K(M)$, $C' = \mathrm{Enc}_K(M')$, $K = \mathrm{KeyGen}()$.

Prove that *no* encryption scheme satisfies this definition.