Cryptography, winter 2013/2014

PROF. DR. JOACHIM VON ZUR GATHEN, DR. DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until Saturday, 25 January 2014, 23:59:59

Exercise 11.1 (Two-time-pad). (5+2 points)

Fix $n \in \mathbb{N}$. Assume two messages $x_1, x_2 \in \mathbb{F}_2^n$ were encrypted with the one-time-pad using the same key k.

(i) Describe which kind of information you can directly obtain from the two encryptions $y_1 = x_1 + k$ and $y_2 = x_2 + k$. $\boxed{1}$

(ii) On the webpage you find two 1000×1000 pixel bitmap images. Find out which objects were depicted on the decrypted images. $\boxed{4}$

(iii) Interpret the results. $\boxed{+2}$

Exercise 11.2 (The (in)security of the RSA signature scheme). (11 points)

Consider the RSA signature scheme (without hashing) and prove the following:

(i) There is an existential forger with key only for the RSA signature scheme. [Hint: Consider $s \in \mathbb{Z}_N^\times$ and compute a message m such that s is a valid signature for m] $\boxed{3}$

(ii) There is an universal forger for the RSA signature scheme that queries two chosen messages. [Hint: Consider messages m, m_1, and m_2 such that $m = m_1 m_2$ in $\mathbb{Z}_N$. Query the signatures for m_1 and m_2 and compute a valid signature of m.] $\boxed{3}$

(iii) There is an existential forger for the RSA signature scheme with chosen messages. $\boxed{2}$

Let h be hash function and consider the hashed RSA signature scheme: For a message m, first hash m and then sign $h(m)$ with RSA.

(iv) Prove: If the hashed RSA signature scheme is existentially unforgeable, then h is inversion resistant. $\boxed{3}$

Exercise 11.3 (The security of the GHR signature scheme). (4 points)

In the lecture we proved that under the strong RSA assumption, GHR signatures are existentially unforgeable with chosen messages. Show that if the GHR forger on messages of length ℓ has success probability at least σ then the reduction succeeds with probability at least $2^{-\ell}\sigma$. $\boxed{4}$