# Cryptography, winter 2013/2014

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

## 10. Exercise sheet
## Hand in solutions until Saturday, 18 January 2014, 23:59:59

**Exercise 10.1** (GHR). (7 points)

Let $p = 6143$ and $q = 6983$. Consider the Gennaro–Halevi–Rabin signature scheme with $\ell = 3$.

(i) Let $P$ be the first $2^\ell$ odd prime numbers and $r = \max(P)$. An RSA modulus $N = pq$ is called *r-safe* if neither $(p-1)/2$ nor $(q-1)/2$ have a prime factor up to $r$. Show whether $N = pq$ is $r$-safe. $\boxed{1}$

(ii) Let $N = pq$ and $t = 42390215$. Now use $(N, \phi(N))$ as secret key and compute the signature for $m = 3$. Verify your signature with the public key $(N, t)$. $\boxed{3}$

(iii) Consider the public key $(32014903, 12345)$ and check which of the following message and signature pairs are valid. $\boxed{3}$

(a) $(4, 17906510)$

(b) $(3, 25088633)$

(c) $(4, 25088633)$

You have encountered several levels of security:

- Impossible Key Recovery,
- Universal Unforgeability,
- Existential Unforgeability;

along with different means for an attacker:

- Key-Only Attack,
- Nonadaptively Chosen-Message Attack,
- Chosen Message Attack.

Pairing an adversarial goal with an attack model defines a security notion.

**Exercise 10.2.** (6+3 points)

Consider the ElGamal signature scheme. Assume that the DL is hard and decide for each of the $9$ security notions whether the scheme is $\boxed{6}$

- ○ secure,
- ○ not secure
- ○ or the answer is unknown.

$\boxed{+3}$ What can you say, if you assume that DL is easy? Use the connections between the security notions to simplify your argument.

**Exercise 10.3.** (4 points)

$\boxed{4}$ For a signature scheme, a message is first hashed and then the hash value is signed. Assume that the signature scheme is existentially unforgeable under the chosen message attack. Does that imply that the hash function is collision resistant? Prove your answer.