Kryptography **Sheet 5**

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 20.11.2023, before the lecture starts

Website: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Exercise 1: Witnesses for compositeness

Show the following assertions.

(a) Each Fermat number $F_n = 2^{2^n} + 1$ passes the Miller–Rabin-test to base 2.

(b) $a = 2$ is a witness for the compositeness of $N = 341$ in Miller–Rabin's test, but not $a = 10$ for the compositeness of $N = 91$.

(c) Why are there always Fermat-witnesses for $N = pq$, $p \neq q$ prime, i.e. a mod N, $(a, N) = 1$, with $a^{N-1} \not\equiv 1$ (N)?

Exercise 2: RSA-attack when using a weak private key

Show: For $q < p < 2q$, p, q prime and $N = pq$ we have $N - \varphi(N) < 3\sqrt{N}$. Furthermore, if $d < N^{1/4}/3$ and $ed \equiv 1$ $(\varphi(N))$ holds, then there exists a $k \in \mathbb{Z}$ with

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

How can the private key d be identified with this information? (Look at chapter Z22 of lecture ZT I.) What does this mean for the security of the RSA-protocol?

Exercise 3: Factorization with sums of two squares

(a) Let N be represented in two different ways as a sum of two squares: $N = s^2 + t^2 = u^2 + v^2$, $s \geq t > 0$, $u \geq v > 0$, $s > u$. Show that $d := (su - tv, N)$ is then a nontrivial divisor of N.

(b) Show: If $N = pq$ with $p \equiv q \equiv 1$ (4), $p \neq q$, then N can be written in two different ways as the sum of two squares. (Look at chapter EZ13 of the lecture EinfZT.)

(c) Can we find a fast factorization algorithm using (b) and (a)?