Kryptography **Sheet 7**

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 04.12.2023, before the lecture starts

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

Exercise 1: On the Miller–Rabin-Condition

(a) Compute all square roots of 1 and -1 mod $n = 2 \cdot 13 \cdot 17 = 442$.

(b) Let $n = 257$ and $a = 17$. Then we have $\varphi(n) = 256 = 2^8 =: 2^s \cdot d$ with $2 \nmid d$, i.e. $s = 8$ and $d = 1$. Compute the smallest $k \in \mathbb{N}$ with $(a^d)^{2^k} \equiv -1 \bmod n$. Why is there no such k, if $n = 221 = 13 \cdot 17$?

Exercise 2: Probability for choosing integers mod n of certain order

Let $n = p_1 \dots p_k$ with pairwise different prime faktors $p_1, \dots, p_k > 2$ and $2^{s_i} \| p_i - 1$ with $s_1 \le s_2 \le \dots \le s_k$. Let P_n be the probability that an arbitrarily chosen $y \in \mathbb{Z}_n^\times$ has even order r, for which $y^{r/2} \not\equiv -1 \bmod n$ holds. Show that

$$P_n = 1 - 2^{-(s_1 + \dots + s_k)} \Big(1 + \frac{2^{s_1 k} - 1}{2^k - 1} \Big)$$

holds, and that this expression is $\ge 1 - 2^{1-k}$.

Exercise 3: Computations in the AES-field

Let be given the AES-field $F = \mathbb{F}_{2^8} := \mathbb{Z}_2[X]/(f)$ with the irreducible polynomial $f(X) := X^8 + X^4 + X^3 + X + 1$. If α denotes the residue class of X in F, we write the elements of F in the shape

(*) $$b_7\alpha^7 + b_6\alpha^6 + \dots + b_1\alpha + b_0$$

with $b_i \in \mathbb{Z}_2 = \{0, 1\}$. While calculating with these elements, α^8 can always be reduced by $\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1$. The coefficients are then abbreviated as **Byte** $b_7 b_6 \dots b_1 b_0$ and interpreted as binary numbers to base 2. For the conversion in the hexadecimal system (base 16), they are represented by two hexadecimal ciphers (`0,1,2,...,9,A,B,C,D,E,F`), e.g. $1 =$`01`, $\alpha =$`02`, $\alpha + 1 =$`03`, $\alpha^2 =$`04` etc.

(a) Give the representation of `05`, ..., `10` in the shape (*).

(b) Compute `10`·`09`, α^{16}, α^{32}, `9A`·`0C` as hexadecimal number.