Hand in: until monday 13.11.2023, before the lecture starts

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

Exercise 1: Coding text in the RSA-protocol

Consider the RSA-modul $n = 22499$ for a RSA-encryption, for which $27^3 \leq n \leq 29^3$ holds, and $n \leq 27^4$.
Plain texts in the plain-text-alphabet A $\mapsto$ 1, ..., Y $\mapsto$ 25, Z $\mapsto$ 0, space $\mapsto$ 26, are split into blocks of three numbers from 0 to 26 each, thus e.g. „KLARTEXT "= 11, 12, 1/ 18, 20, 5/ 24, 20, 26. To each block x_1, x_2, x_3 the number $x = x_1 \cdot 27^2 + x_2 \cdot 27 + x_3$ is assigned, which is encrypted by the RSA-protocol to $v \equiv x^e \bmod n$. The number v will be then described as $v = \tilde{v}_1 \cdot 27^3 + \tilde{v}_2 \cdot 27^2 + \tilde{v}_3 \cdot 27 + \tilde{v}_4$, thus being coded back into the alphabet Σ as a block of four. (a) Let $e = 1291$. Encrypt the plain text message „NACHRICHT". (b) By adding two new symbols, Σ is expanded to Σ', say with the two new symbols "," and ".". By writing $v = v_1 \cdot 29^2 + v_2 \cdot 29 + v_3$, $0 \leq v_i < 29$, $i = 1, 2, 3$, the encrypted text can be represented in the alphabet Σ' by blocks of three. Justify that the plain text can be decrypted uniquely from the encrypted text, using this method. (c) Why is the alphabet-expansion by a single new symbol in (b) not sufficient? (d) Encrypt again the plain text „NACHRICHT" with $e = 1291$ and the expanded secret-text-alphabet Σ' from (b).

Exercise 2: Rules for the discrete logarithm

Consider $(\mathbb{Z}_m^\times, \cdot, 1)$ and let m be such That $\mathbb{Z}_m^\times = \langle g \rangle$ with $g \in \mathbb{Z}_m^\times$. The discrete logarithm is defined by the map

$$\log_g : \begin{cases} \mathbb{Z}_m^\times \to \mathbb{Z}_{\varphi(m)} \\ g^k \bmod m \mapsto k \bmod \varphi(m) \end{cases}$$

Show the following assertions: (a) $\log_g$ is well-defined. (b) $\log_g$ satisfies the functional equation $\log_g(xy) = \log_g(x) + \log_g(y)$ for all $x, y \in \mathbb{Z}_m^\times$. (c) $\log_g$ is bijective. (d) Let m be chosen in such a way, that g, h are primitive roots mod m. Show $\log_h(x) = \log_g(x) \cdot \log_h(g)$ for all $x \in \mathbb{Z}_m^\times$.

Determine a generator g of $\mathbb{Z}_{23}^\times$ and compute $\log_g(13)$.

Exercise 3: Modular square root computation

(a) Let $p \equiv 5\ (8)$ be prime and $a \in \mathbb{Z}$. Show that $X^2 \equiv a \bmod p$ has a pair of solution $\pm x$ with $x = 2^m a^n$ for appropriate $m, n \in \mathbb{N}_0$.

Use this concreteley to compute the solution pair of $X^2 \equiv 13 \bmod 653$.

(b) Compute with method 6.10 of the lecture the roots of $x^2 \equiv 61 \bmod 73$.