Exercise sheet 1

Problem 1

Greek skytale. Formulate a **mathematical** description for the encryption and decryption algorithm of the greek skytale cypher. Do not forget to make clear what the key is. Consider also the case that the length of the message is not divisible by the size of the skytale.

Problem 2

Hill's cipher. Correctness and security are two main features of a cryptosystem. The aim of this problem is to verify the correctness of Hill's cypher.

1. Let R be a commutative ring with unit and $A \in R^{n\times n}$ for some $n \in \mathbb{N}$. Show that A is invertible if and only if $\det(A) \in R^\times$.
2. Let $R = \mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{N}$ and A as above. Show that A is invertible if and only if m and $\det(A)$ seen as an integer are coprime.

Problem 3

Revision of complexity analysis. Let $f, g : \mathbb{N} \to \mathbb{R}$. Prove the following:

(a) $f = \mathcal{O}(f)$.

(b) $c\mathcal{O}(f) = \mathcal{O}(cf) = \mathcal{O}(f)$ for all $c \in \mathbb{R}_{\geq 0}$.

(c) $\mathcal{O}(f)\mathcal{O}(g) = \mathcal{O}(fg)$.

(d) $\log(n!) = \mathcal{O}(n\log(n))$.

Problem 4

Sharing a secret. Let N be a secret that we want to share among k people such that any subset of $k' \leq k$ people can reconstruct N but any $k'-1$ people cannot finde the secret N. The idea is to use the Chinese remainder theorem: Let $a = \lfloor \log_{10}(N)/k' \rfloor + 1$ and choose pairwise coprime numbers n_i such that $10^a \leq n_i \leq 10^{a+1}$ and set $m_i = N \mod n_i$ for $1 \leq i \leq k$ with $0 \leq m_i < n_i$. We distribute the m_i.

(a) Show that any k' people can use their m_i to find N.

(b) How large does N have to be in terms of k and k' such that fewer than k' people cannot obtain the secret?

(c) Is this a secure method?

You may assume that there are plenty of primes in the interval $\left[10^a, 10^{a+1}\right]$, roughly $10^{a+1}/a$.