Exercise 19.
Johnny English wants to prove the British secret service that he knows the factorisation of a composite number $n$ without revealing the factors. These factors are two distinct primes $p$ and $q$ fulfilling $p, q \equiv 3 \pmod{4}$. He suggests the following protocol:

(i) The secret service chooses an arbitrary quadratic residue $y$ modulo $n$, sends $y$ to Johnny.

(ii) Johnny computes the square root $x$ of $y$, sends $x$ to the secret service.

(iii) The secret service checks, whether $x^2 \equiv y \pmod{n}$.

These steps are repeated 20 times, if Johnny can compute the square roots modulo $n$ in all 20 attempts, the secret service believes him. Show that the secret service can factor $n$ with very high probability, hence that this protocol is a zero-knowledge protocol. Is a third party able to derive useful information about the factorisation of $n$ by intercepting the communication between Johnny and the secret service?

Exercise 20.
Zero-knowledge-protocols can also be used to construct signature schemes. Construct a signature scheme from the Feige-Fiat-Shamir identification protocol by replacing the challenge $(b_1, \ldots, b_k)$ with a hash value $h(m, x)$.

Specify the signing and the verification algorithm.

Exercise 21.
In the verification step of the DSA-Signature one first checks, whether $1 \leq r < q$. Show that an attacker can generate signatures for an arbitrary message $m'$ by intercepting just one valid signature $(r, s)$ for a message $m$, if this step is omitted.

Hint: Assume that $h(m)$ is invertible modulo $p - 1$ and modify $r$ and $s$. 