10. Exercise sheet (31.01.2007)

Exercise 10.1 (Discrete Logarithms). Compute the smallest nonnegative solution to the equation $2^x \equiv 3 \pmod{23}$.

Exercise 10.2 (Blind signatures). Particular applications demand a signature protocol between two parties $A$ and $B$ where $B$ signs implicitly a message $m$ on behalf of $A$, but does not know the explicit message he is signing. Thus $B$ cannot associate the message to the user $A$. Such protocols are called blind signatures and play a key role, i.e. in electronic cash schemes and Trusted Computing.

We describe a blinding protocol based on the RSA signature scheme. Let $B$ have the RSA public key $(N, e)$ and secret exponent $d$. In order to receive blind signatures from $B$, party $A$ uses a randomly chosen blinding key $k \in \mathbb{Z}_N^\times$.

(i) Suppose $A$ wants $B$ to sign the message $m \in \mathbb{Z}_N$ or more precisely, wants $B$ to generate a signature from which $A$ can deduce $B$’s signature on $m$. Additionally, $B$ shall not be able to recover $m$. Show that the following protocol fulfills the requirements for a blind signature scheme:

1. $A$ sends $M = m \cdot k^e \in \mathbb{Z}_N$ to $B$.
2. $B$ generates the signature $S(M) = M^d \in \mathbb{Z}_N$ and sends it to $A$.
3. $A$ recovers $S(m) = k^{-1} \cdot S(M) \in \mathbb{Z}_N$. Then $S(m)$ is a valid signature of $m$ by $B$.

(ii) Let $n = p \cdot q$ where $p = 1000000000039$, $q = 10000001000029$ and $e = 2^{16} + 1 = 65537$. Compute the secret exponent $d$ of $B$. Let $k \in \mathbb{Z}_N^\times$ be a random number and $m \in \mathbb{Z}_N$ be the integer value of the ASCII text:

\texttt{blinded}

1. Compute the blinded message $M$.
2. Compute $B$’s blinded signature $S(M)$. What was $B$’s signature on the cleartext $m$?
3. Compute the clear text signature $S(m)$ such as $A$ recovers it using $k$. Compare this signature to $B$’s signature on $m$ computed in (ii.2).