Homework 6 in Cryptography II

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten

19.06.2008

Exercise 15. In the verification step of the ElGamal-Signature one first checks, whether $1 \leq r < p$. Show that an attacker can generate a signature for an arbitrary message m' by intercepting one valid signature (r, s) for a message m, if this step is omitted.

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

Excercise 16. Sign the message with the hash value $h(m) = 18723$ with a simplified DSA siganture. For the public key use $p = 27583, q = 4597, a = 504, y = 23374$. The private key is $x = 1860$.

Afterwards, verify the signature.

Excercise 17. Show that the signature verification of the DSA works.