Lehrstuhl für Theoretische Informationstechnik

Homework 12 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

07.02.2014

Solution to Exercise 34.

Solving this exercise means to execute Algorithm 12.

Algorithm 12 ElGamal signature verification

```
Input: An ElGamal signature $(r, s)$, the corresponding message $m$, a cryptographic hash
  functionh $h$ and the corresponding ElGamal public key $y \in Z_p^*$.
Output: True, if the signature is valid, False otherwise
  Verify that $1 \leq r \leq p - 1$
  $v_1 \leftarrow y^r r^s \mod p$
  $v_2 \leftarrow a^{h(m)} \mod p$
  if $(v_1 = v_2)$ then
      return True
  else
      return False
  end if
```

1) Verify that $1 \leq r \leq p - 1$, i.e., $1 \leq 373 \leq 848$ ✓

2) $v_1 \leftarrow y^r r^s \mod p$

$$y^r = 399^{373} \equiv 672 \text{ and } r^s = 373^{15} \equiv 643 \pmod{859}$$

Both results may be achieved by the SQM-Algorithm.

$$v_1 = 672 \cdot 643 \mod 859 = 19$$

3) $v_2 \leftarrow a^{h(m)} \mod p$

$$v_2 \equiv a^{h(m)} \equiv 206^{65} \equiv 19 \pmod{859}$$

May be achieved by SQM.

4) As $v_1 = v_2$ Algorithm 12 returns True.