Homework 10 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
18.12.2012

Solution to Exercise 31.

(b) One message $m_1 = 567$ is given. We perform a known-plaintext attack.

Let $\boldsymbol{c}_1 = (c_1, c_2)$ and $\boldsymbol{c}_2 = (c_3, c_4)$.

The session key k is the same, since the ciphertexts c_1 and c_3 are congruent:

$$c_1 \equiv c_3 \equiv a^k \pmod{p}.$$

With $y = a^x \pmod{p}$, K is computed by:

$$K = y^k \equiv a^{xk} \mod p,$$

in both cases.

To reveal m_2, we need:

$$m_2 \equiv c_4 K^{-1} \pmod{p}.$$

For known m_1, c_2 and p we can compute K^{-1}:

$$\begin{aligned} m_1 &\equiv K^{-1} c_2 \pmod{p} \\ \Leftrightarrow K^{-1} &\equiv c_2^{-1} m_1 \pmod{p}, \end{aligned}$$

And we finally get:

$$m_2 \equiv c_4 c_2^{-1} m_1 \pmod{p}.$$

For the given values, we have:

$$\begin{aligned} c_2^{-1} &\equiv 347 \pmod{3571}, \\ m_2 &\equiv 1393 \cdot 347 \cdot 567 \pmod{3571} \\ &\equiv 678 \pmod{3571}. \end{aligned}$$