# Exercise 7 in Advanced Methods of Cryptography
# - Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe
2014-12-05

## Solution of Problem 21

Solving this exercise means to execute the Algorithm 12 of the lecture notes.

**Algorithm 12** ElGamal signature verification

**Require:** An ElGamal signature $(r, s)$, the corresponding message $m$, a cryptographic hash function $h$ and the corresponding ElGamal public key $y \in Z_p^*$.
**Ensure:** `True`, if the signature is valid, `False` otherwise

```
Verify that 1 ≤ r ≤ p − 1
v1 ← y^r r^s mod p
v2 ← a^h(m) mod p
if (v1 = v2) 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) Compute $v_1 \leftarrow y^r\, r^s \mod p$:

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

   Both results above can be obtained using the Square-and-Multiply algorithm (SQM). Then $v_1$ yields:

$$v_1 \equiv 672 \cdot 643 \equiv 19 \mod 859.$$

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

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

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

## Solution of Problem 22

We have $p \equiv 3 \mod 4$, $a$ is a primitive element modulo $p$, $y \equiv a^x \mod p$, and $a \mid p-1$.

Assume that it is possible to find $z$ such that $a^{rz} \equiv y^r \mod p$, as given in the description.

Let $s = \frac{p-3}{2}(m - rz)$.

**Task**: Show that $(r, s)$ is a valid signature.

Inserting the provided $s$ yields:

$$\begin{aligned} v_1 &\equiv y^r r^s \equiv a^{rz} r^{\frac{p-3}{2}(m-rz)} \\ &\equiv a^{rz} (r^{\frac{p-3}{2}})^{m-rz} \mod p. \end{aligned} \tag{1}$$

From $a \mid p-1$ if follows that there exits a $v \in \mathbb{Z}$ such that $va = p-1$.

Now, choose $r = v$:

$$ra \equiv p-1 \mod p \Leftrightarrow r \equiv a^{-1}(p-1) \equiv -(a^{-1}) \mod p.$$

To obtain (1), we first substitute $r$ and exponentiate it by the power of $\frac{p-3}{2}$:

$$\Leftrightarrow r^{\frac{p-3}{2}} \equiv (-(a^{-1}))^{\frac{p-3}{2}} \mod p.$$

Note that $(-1) \mod p$ is self-inverse:

$$\Leftrightarrow r^{\frac{p-3}{2}} \equiv \left((-a)^{\frac{p-3}{2}}\right)^{-1} \mod p.$$

For $\frac{p-3}{2}$ even, we obtain $(-1)^{\frac{p-3}{2}} = 1$, and with that:

$$\begin{aligned} \Rightarrow r^{\frac{p-3}{2}} &\equiv \left((-1)^{\frac{p-3}{2}} a^{\frac{p-3}{2}}\right)^{-1} \\ &\equiv (a^{\frac{p-3}{2}})^{-1} \equiv a^{-\frac{p-3}{2}} \\ &\equiv a^{-(\frac{p-1}{2}-1)} \equiv a^{-\frac{p-1}{2}+1} \\ &\equiv \underbrace{a^{-\frac{p-1}{2}}}_{\equiv -1 \mod p} a \equiv -a \mod p. \end{aligned}$$

For the last line, note that $a$ is a primitive element and that $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \mod p$.

This result provides the following for (1):

$$\begin{aligned} v_1 &\equiv y^r r^s \equiv a^{rz} r^{\frac{p-3}{2}(m-rz)} \\ &\equiv a^{rz} (-a)^{(m-rz)} \\ &\equiv a^{rz} a^{m-rz} (-1)^{(m-rz)} \mod p. \end{aligned}$$

Choose $m$ such that $m - rz$ is even valued:

$$\begin{aligned} v_1 &\equiv a^{rz} a^{(m-rz)} \\ &\equiv a^m \equiv v_2 \mod p, \end{aligned}$$

so that the forged signature is valid.

## Solution of Problem 23

In the ElGamal verification $v_1 \equiv v_2 \mod p$ needs to be fulfilled.

Recall that $y = a^x \mod p$ and $r = a^k \mod p$ are used:

$$\begin{aligned} y^r r^s &\equiv a^{h(m)} \mod p \\ \Leftrightarrow a^{xr} a^{ks} &\equiv a^{h(m)} \mod p \\ \overset{\text{Fermat}}{\Leftrightarrow} xr + ks &\equiv h(m) \mod p-1. \end{aligned}$$

Now, we expand both sides of the congruence with $h(m)^{-1}h(m')$:

$$xr \cdot h(m)^{-1}h(m') + ks \cdot h(m)^{-1}h(m') \equiv h(m)h(m)^{-1}h(m') \equiv h(m') \mod p-1 \quad (2)$$

$$\Leftrightarrow xr' + ks' \equiv h(m') \mod p-1 \quad (3)$$

$$\begin{aligned} &\overset{\text{Fermat}}{\Leftrightarrow} a^{xr'} a^{ks'} \equiv a^{h(m')} \mod p \\ &\Leftrightarrow y^{r'} r^{s'} \equiv a^{h(m')} \mod p \\ &\overset{!}{\Leftrightarrow} y^{r'} (r')^{s'} \equiv a^{h(m')} \mod p. \end{aligned}$$

The equivalence assumption in the last line holds if $r \equiv r' \mod p$.

**Note**: In the ElGamal scheme, the condition $1 \le r < p$ must be checked!

From (2) and (3), we have $rh(m)^{-1}h(m') \equiv r' \mod p-1$.

We have to solve the following system of two congruences w.r.t. $r'$:

$$\begin{aligned} r' &\equiv rh(m)^{-1}h(m) \mod p-1, \\ r' &\equiv r \mod p. \end{aligned}$$

By means of the Chinese Remainder Theorem, we get the parameters:

$$\begin{array}{ll} a_1 = r \mod p, & a_2 = rh(m)^{-1}h(m') \mod p-1, \\ m_1 = p, & m_2 = p-1, \\ M_1 = p-1, & M_2 = p, \\ y_1 = M_1^{-1} \equiv p-1 \mod p, & y_2 = M_2^{-1} \equiv 1 \mod p-1, \\ M = p(p-1). & \end{array}$$

The Chinese Remainder Theorem leads to the solution:

$$\begin{aligned} r' &= \sum_{i=1}^{2} a_i M_i y_i = r(p-1)^2 + rh(m)^{-1}h(m')p \\ &\equiv r(p^2 - p - p + 1 + h(m)^{-1}h(m')p) \\ &\equiv r(p(p-1) - p + 1 + h(m)^{-1}h(m')p) \\ &\equiv r(h(m)^{-1}h(m')p - p + 1) \mod M. \end{aligned}$$

The forged signature

$$(r', s') = (r(h(m)^{-1}h(m')p - p + 1) \mod M, sh(m)^{-1}h(m') \mod (p-1))$$

is a valid signature of $h(m')$, if $1 \le r < p$ is not checked.

## Solution of Problem 24

Recall for **a)**, **b)** and **c)** that we have: $r = a^k \mod p$ and $y = a^x \mod p$ from the ElGamal signature scheme.

**a)** This is easily solved by substituting $s = x^{-1}(h(m) - kr)$, $r$ and $y$:

$$\begin{aligned} v_1 \equiv y^s r^r &\equiv y^{x^{-1}(h(m)-kr)} a^{kr} \\ &\equiv a^{xx^{-1}(h(m)-kr)} a^{kr} \\ &\equiv a^{(h(m)-kr)+kr} \\ &\equiv a^{h(m)} \equiv v_2 \mod p. \end{aligned}$$

If the given signature is properly checked, $v_1 = y^s r^r = a^{h(m)} = v_2 \mod p$ is true.

**b)** In this case it is useful to proceed stepwise. We begin with computing:

$$a^s \equiv a^{xh(m)+kr} \equiv a^{xh(m)} a^{kr} \mod p.$$

Next, we substitute $y$ and $r$, correspondingly, and we rearrange the congruence:

$$\begin{aligned} a^s &\equiv y^{h(m)} r^r \mod p \\ \Leftrightarrow a^s r^{-r} &\equiv y^{h(m)} \mod p. \end{aligned}$$

In the last step, we fix the parameters for verification by:

$$\begin{aligned} v_1 &\equiv a^s r^{-r} \mod p, \\ v_2 &\equiv y^{h(m)} \mod p, \end{aligned}$$

so that $v_1 = v_2$ must be checked by the proposed scheme.

**c)** In analogy to **b)**, we compute:

$$\begin{aligned} a^s &\equiv a^{xr+kh(m)} \\ &\equiv a^{xr} a^{kh(m)} \\ &\equiv y^r r^{h(m)} \mod p \\ \Leftrightarrow v_1 = a^s y^{-r} &\equiv r^{h(m)} = v_2 \mod p. \end{aligned}$$