Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 5
- Proposed Solution -

Friday, November 24, 2017

Solution of Problem 1

$$C_i = M_{i+1} \oplus E_K(C_{i-1}), \ \ i = 1, \ldots, n-1 \tag{1}$$

$$\mathrm{MAC}_K^{(n)} = E_K(C_{n-1}) \tag{2}$$

$$C_0 = M_1 \tag{3}$$

$$\hat{C}_i = E_K(\hat{C}_{i-1} \oplus M_i), \ \ i = 1, \ldots, n-1 \tag{4}$$

$$\widehat{\mathrm{MAC}}_K^{(n)} = E_K(\hat{C}_{n-1} \oplus M_n) \tag{5}$$

$$\hat{C}_0 = 0 \tag{6}$$

We show that the equivalency

$$\mathrm{MAC}_K^{(n)} = \widehat{\mathrm{MAC}}_K^{(n)} \tag{7}$$

holds, by induction over n.

Proof. $n = 1$:

$$\mathrm{MAC}_K^{(1)} \overset{(2)}{=} E_K(C_0) \overset{(3)}{=} E_K(M_1) \overset{(6)}{=} E_K(\hat{C}_0 \oplus M_1) \overset{(5)}{=} \widehat{\mathrm{MAC}}_K^{(1)}$$

$n \to n+1$:

$$\begin{aligned}
\mathrm{MAC}_K^{(n+1)} &\overset{(2)}{=} E_K(C_n) \overset{(1)}{=} E_K(M_{n+1} \oplus E_K(C_{n-1})) \\
&\overset{(2)}{=} E_K\left(M_{n+1} \oplus \mathrm{MAC}_K^{(n)} \right) \\
&\overset{(7)}{=} E_K\left(M_{n+1} \oplus \widehat{\mathrm{MAC}}_K^{(n)} \right) \\
&\overset{(5)}{=} E_K\left(M_{n+1} \oplus E_K\left(\hat{C}_{n-1} \oplus M_n \right) \right) \\
&\overset{(4)}{=} E_K\left(M_{n+1} \oplus \hat{C}_n \right) \overset{(4)}{=} \hat{C}_{n+1} = \widehat{\mathrm{MAC}}_K^{(n+1)}
\end{aligned}$$

$\square$

Solution of Problem 2

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:

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

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

$$xr \cdot h(m)^{-1}h(m') + ks \cdot h(m)^{-1}h(m') \equiv h(m)h(m)^{-1}h(m') \equiv h(m') \mod p - 1 \quad (8)$$
$$\Leftrightarrow xr' + ks' \equiv h(m') \mod p - 1 \quad (9)$$
$$\overset{\text{Fermat}}{\Leftrightarrow} a^{xr'} a^{ks'} \equiv a^{h(m')} \mod p$$
$$\Leftrightarrow y^{r'} r^{s'} \equiv a^{h(m')} \mod p$$
$$\overset{!}{\Leftrightarrow} y^{r'} (r')^{s'} \equiv a^{h(m')} \mod p.$$

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

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

From (8) and (9), 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':

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

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

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

The Chinese Remainder Theorem leads to the solution:

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

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 $1 \leq r < p$ is not checked.

Solution of Problem 3

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:

$$v_1 \equiv y^r r^s \equiv a^{rz} r^{\frac{p-3}{2}(m-rz)}$$

$$\equiv a^{rz} (r^{\frac{p-3}{2}})^{m-rz} \mod p. \tag{10}$$

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 (10), 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:

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

$$\equiv (a^{\frac{p-3}{2}})^{-1} \equiv a^{-\frac{p-3}{2}}$$

$$\equiv a^{-(\frac{p-1}{2}-1)} \equiv a^{-\frac{p-1}{2}+1}$$

$$\equiv \underbrace{a^{-\frac{p-1}{2}}}_{\equiv -1 \mod p} a \equiv -a \mod p.$$

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 (10):

$$v_1 \equiv y^r r^s \equiv a^{rz} r^{\frac{p-3}{2}(m-rz)}$$

$$\equiv a^{rz}(-a)^{(m-rz)}$$

$$\equiv a^{rz} a^{m-rz}(-1)^{(m-rz)} \mod p.$$

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

$$v_1 \equiv a^{rz} a^{(m-rz)}$$

$$\equiv a^m \equiv v_2 \mod p,$$

so that the forged signature is valid.