Dr. Michael Reyer

Tutorial 5
- Proposed Solution -

Friday, November 23, 2018

Solution of Problem 1

$$
\begin{aligned}
C_i &= M_{i+1} \oplus E_K(C_{i-1}), \quad i = 1, \dots, n-1 && (1)\\
\mathrm{MAC}_K^{(n)} &= E_K(C_{n-1}) && (2)\\
C_0 &= M_1 && (3)\\
\hat{C}_i &= E_K(\hat{C}_{i-1} \oplus M_i), \quad i = 1, \dots, n-1 && (4)\\
\widehat{\mathrm{MAC}}_K^{(n)} &= E_K(\hat{C}_{n-1} \oplus M_n) && (5)\\
\hat{C}_0 &= 0 && (6)
\end{aligned}
$$

We show that the equivalency

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

holds, by induction over n.

Proof. $n = 1$:

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

$n \to n+1$:

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

□

Solution of Problem 2

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

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

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

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

$$x\,r\,u + k\,s\,u \equiv h(m)h(m)^{-1}h(m') \equiv h(m') \pmod{p-1} \quad (8)$$

$$\Leftrightarrow xr' + ks' \equiv h(m') \pmod{p-1} \quad (9)$$

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

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

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

From (8) and (9), we have $r\,u \equiv r' \pmod{p-1}$.

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

$$\begin{aligned} r' &\equiv r\,u \pmod{p-1}, \\ r' &\equiv r \pmod p. \end{aligned}$$

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

$$\begin{aligned} &a_1 = r \mod p, && a_2 = r\,u \mod (p-1), \\ &m_1 = p, && m_2 = p-1, \\ &M_1 = p-1, && M_2 = p, \\ &y_1 = M_1^{-1} \equiv p-1 \pmod p, && y_2 = M_2^{-1} \equiv 1 \pmod{p-1}, \\ &M = p(p-1). \end{aligned}$$

The Chinese Remainder Theorem leads to the solution:

$$\begin{aligned} r' &= \textstyle\sum_{i=1}^{2} a_i M_i y_i = r(p-1)^2 + r\,u\,p \\ &\equiv r(p^2 - p - p + 1 + u\,p) \\ &\equiv r(p(p-1) - p + 1 + u\,p) \\ &\equiv r(u\,p - p + 1) \pmod{M = p(p-1)}. \end{aligned}$$

The forged signature

$$(r', s') \text{ with } r' = r(u\,p - p + 1) \mod M, \text{ and } s' = s\,u \mod (p-1)$$

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

Solution of Problem 3

We have $p \equiv 3 \pmod 4$, a is a primitive element modulo p, $y = a^x \mod p$, and $a \mid p-1$. Assume that it is possible to find z such that $a^{rz} \equiv y^r \pmod p$, as given in the description. Let $s = \frac{p-3}{2}(h(m) - rz) \mod p-1$. From $a \mid p-1$ if follows that there exits a $v \in \mathbb{Z}$ such that $va = p-1$.

Choose $r = v$.

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

Inserting the provided s yields:

$$\begin{aligned} v_1 \equiv y^r r^s &\equiv a^{rz} r^{\frac{p-3}{2}(h(m)-rz)} \\ &\equiv a^{rz}(r^{\frac{p-3}{2}})^{h(m)-rz} \pmod p. \end{aligned} \tag{10}$$

Furthermore,

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

To obtain (10), we exponentiate the above equation by the power of $\frac{p-3}{2}$:

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

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

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

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

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

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

This result provides the following for (10):

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

As m is chosen such that $h(m) - rz$ is even:

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

so that the forged signature is valid.