Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 13
- Proposed Solution -

Friday, July 22, 2016

Solution of Problem 1

As given, we have the parameters $a, b \in \mathbb{Z}$ and $a', b' \in \mathbb{Z}$. Furthermore, we have $M = ab - 1$, the private key $d = b'M + b$, and the public key (n, e) with $e = a'M + a$, and $n = \frac{ed-1}{M}$. By substitution we obtain the following for n:

$$\begin{aligned} n &= \frac{ed-1}{M} \\ &= \frac{(a'M+a)(b'M+b)-1}{M} \\ &= \frac{a'b'M^2 + a'bM + ab'M + ab - 1}{M} \\ &= a'b'M + a'b + ab' + 1. \end{aligned}$$

a) The encryption operation is computing $c \equiv em \mod n$. The decryption operation is computing $dc \mod n$. From $dc \equiv dem \mod n \overset{!}{\equiv} m \mod n$, it follows that $de \equiv 1 \mod n$ must hold:

$$\begin{aligned} de &\equiv (a'M+a)(b'M+b) \mod n \\ &\equiv a'b'M^2 + ab'M + a'bM + ab \mod (a'b'M + ab' + ba' + 1) \\ &\equiv 1 \mod (a'b'M + ab' + ba' + 1). \end{aligned}$$

For the given system, $de \equiv 1 \mod n$ is always true.

b) We consider an attack to break the private key d. Note that c, n, e are public. Furthermore, since $de \equiv 1 \mod n$ holds, it follows that $\gcd(de, n) = 1$. We can compute the inverse of e modulo n using the Euclidean algorithm. As $e^{-1} \equiv d \mod n$ holds, the private key is easily computed using the Euclidean algorithm.

Solution of Problem 2

a) Apply the encryption function.

$$\begin{aligned} n &= p \cdot q = 199 \cdot 211 = 41989\,, \\ c &= e_K(32767) = m \cdot (m + B) \mod n \\ &= 32767 \cdot (32767 + 1357) \mod 41989 \\ &\equiv 16027 \mod 41989 \end{aligned}$$

b) Start with the encryption function and solve for m.

$$\begin{aligned} c &\equiv m^2 + B \cdot m \mod n \\ c + \left(\frac{B}{2}\right)^2 &\equiv m^2 + B \cdot m + \left(\frac{B}{2}\right)^2 \mod n \\ c + \left(\frac{B}{2}\right)^2 &\equiv \left(m + \frac{B}{2}\right)^2 \mod n \end{aligned}$$

Using the Extended Euclidean Algorithm, the multiplicative inverse of 2 modulo n is calculated as $2^{-1} \equiv 20995 \mod 41989$. With

$$\begin{aligned} \tilde{c} &:= c + \left(\frac{B}{2}\right)^2 \mod n \\ &\equiv 16027 + (1357 \cdot 20995)^2 \mod n \\ &\equiv 4013 \mod n\,, \end{aligned}$$

and

$$\begin{aligned} \tilde{m} &:= m + \frac{B}{2} \mod n \\ &\equiv m + 1357 \cdot 20995 \mod n \\ &\equiv m + 21673 \mod n\,, \end{aligned}$$

we can conclude

$$\begin{aligned} \tilde{c} &\equiv \tilde{m}^2 \mod n \\ 4013 &\equiv \tilde{m}^2 \mod n\,. \end{aligned}$$

This form is the standard Rabin Cryptosystem. In order to find the square root modulo n, we use Proposition 9.4. First, find

$$1 = \underbrace{s \cdot p}_{=:b} + \underbrace{t \cdot q}_{=:a}$$

using the Extended Euclidean Algorithm.

$$\begin{aligned} 211 &= 1 \cdot 199 + 12 \\ 199 &= 16 \cdot 12 + 7 \\ 12 &= 1 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ \Rightarrow 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (12 - 1 \cdot 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 \\ &= 3 \cdot 12 - 5 \cdot (199 - 16 \cdot 12) = 83 \cdot 12 - 5 \cdot 199 \\ &= 83 \cdot (211 - 1 \cdot 199) - 5 \cdot 199 = 83 \cdot 211 - 88 \cdot 199 \\ \Rightarrow b &= -88 \cdot 199 = -17512 \\ a &= 83 \cdot 211 = 17513 \end{aligned}$$

Next, we calculate the square roots modulo p and q (this is Proposion 9.3).

$$\begin{aligned}
x^2 &\equiv 4013 \equiv 33 \mod p \\
\Rightarrow x_1 &= 33^{\frac{p+1}{4}} = 33^{50} \equiv 86 \mod 199 \\
x_2 &= -x_1 \equiv 113 \mod 199\,, \\
y^2 &\equiv 4013 \equiv 4 \mod q \\
\Rightarrow y_1 &= 4^{\frac{q+1}{4}} = 4^{53} \equiv 209 \mod 211 \\
y_2 &= -y_1 = 2 \mod 211
\end{aligned}$$

Then, $f_{x_i,y_j} = ax_i + by_j$ are solutions to $f^2 = 4013 \mod n$.

$$\begin{aligned}
f_{x_1,y_1} &= a \cdot x_1 + b \cdot y_1 \mod n \\
&\equiv 17513 \cdot 86 - 17512 \cdot 209 \mod 41989 \\
&\equiv 36503 - 6965 \mod 41989 \\
&\equiv 29538 \mod 41989 \\
f_{x_1,y_2} &= 17513 \cdot 86 - 17512 \cdot 2 \mod 41989 \\
&\equiv 36503 - 35024 \mod 41989 \\
&\equiv 1479 \mod 41989 \\
f_{x_2,y_1} &= 17513 \cdot 113 - 17512 \cdot 209 \mod 41989 \\
&\equiv 5486 - 6965 \mod 41989 \\
&\equiv 40510 \equiv -f_{x_1,y_2} \mod 41989 \\
f_{x_2,y_2} &= 17513 \cdot 113 - 17512 \cdot 2 \mod 41989 \\
&\equiv 5486 - 35024 \mod 41989 \\
&\equiv 12451 \equiv -f_{x_1,y_1} \mod 41989
\end{aligned}$$

With

$$\begin{aligned}
\tilde{m}^2 &\equiv \tilde{c} \mod n \\
\tilde{m} &\equiv f_{x_i,y_j} \mod n \\
m_{x_i,y_j} + 21673 &\equiv f_{x_i,y_j} \mod n \\
m_{x_i,y_j} &\equiv f_{x_i,y_j} - 21673 \mod n
\end{aligned}$$

the four possible messages can now be calculated.

$$\begin{aligned}
m_{x_1,y_1} &= 29538 - 21673 \equiv 7865 \mod n \\
m_{x_1,y_2} &= 1479 - 21673 \equiv 21795 \mod n \\
m_{x_2,y_1} &= 40510 - 21673 \equiv 18837 \mod n \\
m_{x_2,y_2} &= 12451 - 21673 \equiv 32767 \mod n
\end{aligned}$$

Message m_{x_2,y_2} is the original one, but, knowing only the cryptogram and the private key, this message cannot be identified as the original one.

Solution of Problem 3

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 $h(m)^{-1}h(m')$:

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

$$\Leftrightarrow xr' + ks' \equiv h(m') \mod p-1 \quad (2)$$

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

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 (1) and (2), 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:

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

The Chinese Remainder Theorem leads to the solution:

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

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.