Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Review
- Proposed Solution -

Tuesday, March 15, 2016

Solution of Problem 1

a) $p = 13$ is a prime number, $a = 5$ is a quadratic residue mod p.

1) $v = b^2 - 4a = b^2 - 4 \cdot 5 = b^2 - 20$.

   Choose: $b = 5 \Rightarrow v = 25 - 20 = 5$.
   With Euler's criterion, compute: $(\frac{v}{p}) = (\frac{5}{11}) = 5^{\frac{10}{2}} = 1$.
   $\Rightarrow v = 5$ is a quadratic residue mod 11. $\lightning$

   Choose: $b = 6 \Rightarrow v = 36 - 20 = 16 \equiv 5 \mod 11$.
   $\Rightarrow v = 5$ is a quadratic residue mod 11. $\lightning$

   Choose: $b = 7 \Rightarrow v = 49 - 20 = 29 \equiv 7 \mod 11$.
   With Euler's criterion, compute:
   $(\frac{7}{11}) = 7^{\frac{p-1}{2}} \equiv 7^{\frac{10}{5}} \equiv 7^5 \equiv 49 \cdot 49 \cdot 7 \equiv 5 \cdot 5 \cdot 7 \equiv -1 \mod 11$.
   $\Rightarrow v$ is a quadratic non-residue modulo 11. ✓

2) Insert the values for a and b into the polynomial $f(x) = x^2 - 7x + 5$.

3) Compute $r = x^{\frac{p+1}{2}} \mod f(x)$:

$$
\begin{array}{l}
x^6 : (x^2 - 7x + 5) = x^4 + 7x^3 + 2x - 3 \\
\underline{-\,(x^6 - 7x^5 + 5x^4)} \\
+\,7x^5 - 5x^4 \\
\underline{-\,(7x^5 - 5x^4 + 2x^3)} \\
-\,2x^3 \\
\underline{-\,(-2x^3 + 3x^2 - 10x)} \\
-\,3x^2 + 10x \\
\underline{-\,(-3x^2 + 10x - 4)} \\
4
\end{array}
$$

   Hence, $r = 4$. Furthermore, and $-r = -4 \equiv 7 \mod 11 \Rightarrow (r, -r) = (4, 7)$.
   // Validation $r^2 = a \mod 11$ is correct in both cases.

b) Both p, q satisfy the requirement for a Rabin cryptosystem: $p, q \equiv 3 \mod 4$.
For $c \mod p \equiv 225 \mod 11 \equiv 5$, we already know the square roots $x_{p,1} = 4$, $x_{p,2} = 7$.

For $c \mod q \equiv 225 \mod 23 \equiv 18$, compute the square roots $x_{q,1}$, $x_{q,2}$ with the auxiliary parameter $k_q = \frac{q+1}{4} = 6$:

$$x_{q,1} = c^{k_q} = 18^6 = 18^3 \cdot 18^3 \equiv 13 \cdot 13 \equiv 8 \mod 23,$$
$$x_{q,2} = -8 \equiv 15 \mod 23.$$

Formulate $tq + sp = 1$:

$$23 = 2 \cdot 11 + 1$$
$$\Rightarrow 1 = 23 - 2 \cdot 11$$

We set $a = tq = 23$ and $b = sp = -22$. Compute all four possible solutions:

$$m_{11} = ax_{p,1} + bx_{q,1} = 23 \cdot 4 - 22 \cdot 8 = -84 \equiv 169 \mod 253 \Rightarrow (...1001)_2 \quad \lightning$$
$$m_{12} = ax_{p,1} + bx_{q,2} = 23 \cdot 4 - 22 \cdot 15 = -238 \equiv 15 \mod 253 \Rightarrow (...1111)_2 \quad \lightning$$
$$m_{21} = ax_{p,2} + bx_{q,1} = 23 \cdot 7 - 22 \cdot 8 = -15 \equiv 238 \mod 253 \Rightarrow (...1110)_2 \quad \lightning$$
$$m_{22} = ax_{p,2} + bx_{q,2} = 23 \cdot 7 - 22 \cdot 15 = -169 \equiv 84 \mod 253 \Rightarrow (...0100)_2 \quad \checkmark$$

The solution is $m = m_{21} = 84$ since it ends on 0100 in the binary representation.
// Checking all solutions yields $c = 225$.

c) Since $c = 225$, on can to compute two square roots in the reals, $m = \pm 15$. If Nelson chooses 1111, the result $m = 15$ is obvious, without knowing the factors in $n = pq$.

Solution of Problem 2

a) Easy to compute, preimage resistant, 2nd preimage resistant, collision-free.

b) Given, $h(m) = m^2 - 1 = (m+1)(m-1) \mod L$. Let $m' = m + kL$ with $k \in \mathbb{N}$. $h(m') = (m'+1)(m'-1) = (m+kL+1)(m+kL-1) \equiv (m+1)(m-1) \mod L = h(m)$.

c) $k_0 = 57$, $k_1 = 6, k_2 = 36, k_3 = 27, k_4 = 24, k_5 = 12, k_6 = 3, k_7 = 9, k_8 = 34$

d) For $m = 10$ we obtain the bitstream $\hat{m} = 01010$ (with $n = 5$ bits).
The number of zeros is 3 and $t = 5 + \lfloor \log_2(5) \rfloor + 1 = 8$.
This leads to the concatenated message:

$$\hat{w} = 01010|011 = (a_1, ..., a_5)||(a_6, ..., a_8).$$

The positions with $a_j = 1$ are $2, 4, 7, 8$.
The signature for $m = 10$ is: $(k_2, k_4, k_7, k_8) = (36, 24, 9, 34)$.

The public keys needed for this message are v_2, v_4, v_7, v_8.
The signature is correct since $(v_2, v_4, v_7, v_8) = (h(k_2), h(k_4), h(k_7), h(k_8))$ holds.

e) Eve can generate signatures for arbitrary messages as soon as all keys have been used at least once. After Alice has signed a message, some keys are available for Eve so that she can already sign some messages.

Solution of Problem 3

Schnorr Identification Scheme Solution

(a) Discrete Logarithm.

(b)

$$\begin{aligned} \beta^y v^r &\equiv \beta^{k+ar} v^r && \mod p \\ &\equiv \beta^{k+ar} \beta^{-ar} && \mod p \\ &\equiv \beta^k && \mod p \\ &\equiv \gamma && \mod p \end{aligned}$$

(c) A random number needs to be generated first. Step 1 requires an exponentiation modulo p. Step 3 comprises one additon and one multiplication modulo p.

The modular exponentiation is computationally intensive, but this can be precomputed offline, before the scheme is executed. That means the scheme is designed such that is can be fast even if Alice uses a smartcard.

(d)

$$v = \beta^{-a} = (\beta^a)^{-1} = (20^5)^{-1} \equiv 30^{-1} \equiv 45 \mod 71$$
$$\gamma = \beta^k = 20^{10} \equiv 48 \mod 71$$
$$y = k + ar = 10 + 5 \cdot 4 \equiv 2 \mod 7$$
$$\gamma = 48 \overset{!}{\equiv} \beta^y v^r = 20^2 45^4 = 48 \mod 71 \checkmark$$

Solution of Problem 4

Elliptic Curves Solution

(a)

$$\begin{aligned}
\Delta &= -16(4a^3 + 27b^2) && \mod 7 \\
&= -16(4a^3 + 27 \cdot 2^2) && \mod 7 \\
&= -16(4a^3 + 108) && \mod 7 \\
&\equiv 5(4a^3 + 3) && \mod 7 \\
&= 20a^3 + 15 && \mod 7 \\
&\equiv 6a^3 + 1 \overset{!}{\not\equiv} 0 && \mod 7
\end{aligned}$$

$$\begin{aligned}
\Rightarrow \quad & 6a^3 \not\equiv -1 && \mod 7 \\
\Leftrightarrow \quad & 6a^3 \not\equiv 6 && \mod 7 \\
\Leftrightarrow \quad & a^3 \not\equiv 1 && \mod 7 \\
\Rightarrow \quad & a \in \{0, 3, 5, 6\} && \mod 7
\end{aligned}$$

(b) Begin by filling out the following table.

z	z^{-1}	$3z$	z^2	z^3	$z^3 + 3z + 2$
0	-	0	0	0	2
1	1	3	1	1	6
2	4	6	4	1	2
3	5	2	2	6	3
4	2	5	2	1	1
5	3	1	4	6	2
6	6	4	1	6	5

From the table we get

$$E_3(\mathbb{F}_7) = \{(0,3), (0,4), (2,3), (2,4), (4,1), (4,6), (5,3), (5,4), \mathcal{O}\}\,.$$

The inverses are calculated as

$$\begin{aligned}
(0,3) &= -(0,4) \\
(0,4) &= -(0,3) \\
(2,3) &= -(2,4) \\
(2,4) &= -(2,3) \\
(4,1) &= -(4,6) \\
(4,6) &= -(4,1) \\
(5,3) &= -(5,4) \\
(5,4) &= -(5,3) \\
\mathcal{O} &= -\mathcal{O}\,.
\end{aligned}$$

(c) $\#E_3(\mathbb{F}_7) = 9$

(d) With group law addition, $E_3(\mathbb{F}_7)$ is a finitie abelian group. It holds $\text{ord}(P) \mid \#E(\mathbb{F}_7)$ (Lagrange's theorem). In this case, it follows for $P \neq 0 : 1 < \text{ord}(P) = \{3, 9\}$, i.e., a point in the group generates a subgroup of either size three or nine. We have to show that the point $(0, 3)$ does not generate a subgroup of size three. It is then a generator of the group.

$$
\begin{aligned}
&1P = (0,3)\\
&2P = (0,3) + (0,3) = (x,y) = (2,3)\\
&\quad \text{with}\\
&\quad c = \frac{3 \cdot 0^2 + 3}{2 \cdot 3} = \frac{1}{2} = 4 \mod 7\\
&\quad x = c^2 - 2 \cdot 0 = 4^2 \equiv 2 \mod 7\\
&\quad y = c(0-2) - 3 = -2 \cdot 4 - 3 = -11 \equiv 3 \mod 7\\
&3P = (2,3) + (0,3) = \neq \mathcal{O} \text{ ((2,3) is not the inverse of (0,3).)}
\end{aligned}
$$

It follows that $(0, 3)$ is a generator of the group.

(e) A trivial upper bound is $2q + 1$. A trivial lower bound is 1. Alternatively, with Hasse, the bounds become:

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$