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

Exercise 11
- Proposed Solution -

Friday, January 26, 2018

Solution of Problem 1

a) $E_\alpha : Y^2 = X^3 + \alpha X + 1$ in $\mathbb{F}_{13}$.

$$\alpha = 2$$
$$\Delta = -16(4a^3 + 27b^2) = 10(4 \cdot 2^3 + 27) = 10 \cdot 59 \equiv 5 \not\equiv 0 \mod 13$$

$\Rightarrow E_2$ is an elliptic curve.

b)

$$0P = \mathcal{O}$$
$$1P = (0,1)$$
$$2P = (0,1) + (0,1) = (1,11)$$
$$\text{using } x_3 = \left(\frac{3 \cdot 0^2 + 2}{2 \cdot 1}\right)^2 - 2 \cdot 0 = (2 \cdot 2^{-1})^2 = 1$$
$$y_3 = 1 \cdot (0 - 1) - 1 = -2 = 11$$
$$3P = (1,11) + (0,1) = (8,10)$$
$$\text{using } x_3 = \left(\frac{1 - 11}{0 - 1}\right)^2 - 1 - 0 = (3 \cdot 12)^2 - 1 = 36^2 - 1 = 8$$
$$y_3 = 36(1 - 8) - 11 = 10$$
$$4P = (8,10) + (0,1) = (2,0)$$
$$\text{using } x_3 = \left(\frac{1 - 10}{0 - 8}\right)^2 - 8 - 0 = (4 \cdot 5^{-1})^2 - 8 = (4 \cdot 8)^2 - 8 = 2$$
$$y_3 = 20(8 - 0) - 3 = 1$$

c) $\langle P \rangle \subseteq \{\mathcal{O}, (0,1), (1,11), (8,10), (2,0), (0,12), (1,2), (8,3)\}$, where $(0,1) = -(0,12)$, $(1,11) = -(1,2)$, $(8,10) = -(8,3)$ and $(2,0) = -(2,0)$. We start with the five points calculated earlier. Then we add the inverse elements, as they must be elements of the subgroup. With $\#\langle P \rangle = \#E(\mathbb{F}_{13})$ is P a cyclic generator of order $\#\langle P \rangle = 8$.

Note: equivalent solutions are possible.

d) With $b_i = iP$, $a = jm + i$, $g_j = Q - jmP$

$$b_i = g_j \Leftrightarrow iP = Q - jmP \Leftrightarrow Q = (i + jm)P \Leftrightarrow Q = aP$$

$i + mj$ covers all numbers between $0, \ldots, q - 1$.

e) The *babysteps* have already been computed. Compute *giantsteps*: $Q - jmP$ until $Q - jmP = iP$ for some i with $j = 0, \ldots, m-1$.

$$\begin{aligned} j = 0 &: (8,3) - 0(2,0) = (8,3) \\ j = 1 &: (8,3) - (2,0) = (8,3) + (2,0) = (0,1) = P \\ \text{with } x_3 &= \left(\frac{0-3}{2-8}\right)^2 - 8 - 2 = (10 \cdot 2)^2 - 10 = 0 \\ y_3 &= 20(8-0) - 3 = 1 \end{aligned}$$

$$\begin{aligned} \Rightarrow & j = 1, i = 1 \\ \Rightarrow & k = i + jm = 1 + 1 \cdot 4 = 5 \\ & Q = 5P \Rightarrow 5(0,1) = (8,3) \end{aligned}$$

Check:

$$\begin{aligned} 5P = 4P + P &= (2,0) + (0,1) = (8,3) \\ \text{using } x_3 &= \left(\frac{1-0}{0-2}\right)^2 - 1 - 0 = 16^2 - 2 = 8 \\ y_3 &= (1 \cdot 6)(2-8) - 0 = 6 \cdot 7 - 0 = 42 = 3 \end{aligned}$$

Solution of Problem 2

(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)

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

Solution of Problem 3

a) We have $\alpha = (5n + 7)$ and $\beta = (3n + 4)$ **(3P)**

The Bezout lemma states that iff a and b are coprime then the following equation has integer solutions:

$$\alpha \cdot x + \beta \cdot y = 1$$

Therefore,

$$(5n + 7) \cdot x + (3n + 4) \cdot y = 1$$

Now, we apply the EEA to the previous equation:

$$\begin{aligned}(5n + 7) &= (3n + 4) + (2n + 3)\\ (3n + 4) &= (2n + 3) + (n + 1)\\ (2n + 3) &= 2(n + 1) + 1\end{aligned}$$

Now backwards:

$$\begin{aligned}1 &= (2n + 3) - 2(n + 1)\\ &= (2n + 3) - 2(-(2n + 3) + (3n + 4))\\ &= 3(2n + 3) - 2(3n + 4)\\ &= (2n + 3) + 2(2n + 3) - 2(3n + 4)\\ &= 3(2n + 3) - 2(3n + 4)\\ &= 3((5n + 7) - (3n + 4)) - 2(3n + 4)\\ &= 3(5n + 7) - 3(3n + 4) - 2(3n + 4)\\ &= 3(5n + 7) - 5(3n + 4)\end{aligned}$$

Therefore, $x = 3$ and $y = -5$ which prove that α and β are relatively prime

b) The steps to generate the first prime p are the following: **(3P)**

- Using a random number generator, we generate a random number of size $K/2$
- Set the lowest bit of the generated integer to ensure that the number will be odd
- Set the two highest bits of the integer to ensure that the highest bits of n will be set
- Using the MRPT, we check if the resulting integer is prime. If not, we increment the value by 2 and check again

The entire procedure is analogous for q.

c) The given RSA cryptosystem has the following parameters: **(3P)**

$p = 11$, $q = 13$, $e = 7$ and $n = p \cdot q = 143$

Using the Euler function: $\phi(n) = 10 \cdot 12 = 120$

Having the expression: $m = c^d \bmod n$, we need to calculate the $gdc(e, \phi(n)) = 1$

$$120 = 17 \cdot 7 + 1$$
$$7 = 1 \cdot 6 + 1$$

Now backwards

$$\begin{aligned} 1 &= 7 - (1 \cdot 6) \\ &= 7 - 6(120 - 17 \cdot 7) \\ &= 7 - (6 \cdot 120) + 102 \cdot 7 \\ &= 103 \cdot 7 - 6 \cdot 120 \longrightarrow d = 103 \end{aligned}$$

$m \equiv c^d \bmod n \equiv 31^{103} \bmod 143$. Therefore, applying the SM algorithm we obtain $m = 47$

d) Since $gcd(e_A, e_B) = 1$, there exist integers x and y with $e_A \cdot x + e_B \cdot y$. Therefore, $m = m^1 = m^{e_A \cdot x + e_B \cdot y} = (m^{e_A})^x \cdot (m^{e_B})^y \equiv {c_A}^x \cdot {c_B}^y$. Since Claire has access to the values c_A and c_B she can calculate m. **(2P)**

e) The requirements of a digital signature are: **(2P)**

- it must be verifiable
- it must be forgery-proof
- it must be firmly connected to the document

f) Oskar wants to obtain a chosen signature $s = m^d \bmod n$ **(2P)**

- Oskar generates a message $m_2 = m \cdot m^{-1} \bmod n$ and asks again to sign a message m_2, obtaining $s_2 = {m_2}^d \bmod n$
- From the pairs (m_1, s_1) and (m_2, s_2) the wanted signature s on message m can be recovered as $s = s_1 \cdot s_2 \bmod n$

Proof :

$$\begin{aligned} s \equiv s_1 \cdot s_2 \equiv {m_1}^d \cdot {m_2}^d \equiv {m_1}^d \cdot (m \cdot m^{-1})^d \equiv \\ \equiv {m_1}^d \cdot m^d \equiv m^d \mathrm{mod} n \end{aligned}$$