Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

Tutorial 0
- Proposed Solution -

Wednesday, March 4, 2015

Solution of Problem 1

a) A quadratic residue (QR) modulo $p \Leftrightarrow \exists b \in \mathbb{Z}_p$ with $b^2 \equiv a \mod p$.
It holds $d^2 \equiv (a^{\frac{p-1}{4}})^2 \equiv (b^2)^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \mod p$ by Fermat.
It is $(d^2-1) = (d-1)(d+1)$, as $\mathbb{Z}_n$ is a field, and it follows $d \equiv 1$ or $d \equiv -1 \mod p$.

b) We consider the two cases of $d = \pm 1$:

Case $d = 1 \Rightarrow r^2 \equiv (a^{\frac{p+3}{8}})^2 \equiv a^{\frac{p+3}{4}} \equiv (a^{\frac{p-1}{4}})a \equiv da \equiv a \mod p$

Case $d = -1 \Rightarrow r^2 \equiv (2a(4a)^{\frac{p-5}{8}})^2 \equiv 4a^2(4a)^{\frac{p-5}{4}} \equiv a(4a)^{\frac{p-1}{4}} \equiv a(2^{\frac{p-1}{2}})(a^{\frac{p-1}{4}}) \equiv a(-1)d \equiv a(-1)(-1) \equiv a \mod p$

As $r^2 \equiv a \mod p$ holds in both cases, $(r, -r)$ are the only square roots of $a \mod p$.

c) The parameters yield $p = 53 = 5 + 6 \cdot 8 \equiv 5 \mod 8$ and $q = 37 = 5 + 4 \cdot 8 \equiv 5 \mod 4$.
$\Rightarrow$ Algorithm SQR can be applied to compute the square roots:
$d_p \leftarrow a^{\frac{p-1}{4}} \mod p$

$$d_p \equiv 17^{13} \equiv 17((17)^4)^3 \equiv 17(46)^3 \equiv 17 \cdot 28 \equiv 52 \equiv -1$$
$$d_q \equiv 10^9 \equiv 1 \mod 37$$

$$d_p = -1 \Rightarrow r_p \equiv 34(68)^6 34(15^6) \equiv 34 \cdot 24 \equiv 21 \mod 53$$
$$d_q = 1 \Rightarrow r_q \equiv 10^5 26 \mod 37$$

The square roots of 17 modulo 53 are 21 and 32.
The square roots of 10 modulo 37 are 11 and 26. Alternatively, use SQM: $13 = (1101)_2$ and compute $17^{13} \mod 53$:

i	b_i	x	x^2	$17x^2$
2	1	17	24	37
1	0	3	44	-
0	1	44	28	52

d) It is given: $7 \cdot 53 - 10 \cdot 37 = 1 = sp + tq = b + a = 371 - 370$
Then, all possible solutions for the message are given as: $\pm ax \pm by$, where x is the square root of $c = 1342 \mod p$, and y is the square root of $c = 1342 \mod q$.

$1342 \mod 53 = 17$ and $1342 \mod 37 = 10$ such that the square roots are given in (c) as 21 and 11, respectively. $n = pq = 53 \cdot 37 = 1961$.

$$\begin{aligned}
f_1 &= -370 \cdot 21 + 371 \cdot 11 = -7770 + 4081 \equiv 74 + 159 \equiv 233 \Rightarrow (...001)_2 \\
f_2 &= -370 \cdot 21 - 371 \cdot 11 = 74 - 159 \equiv 1876 \Rightarrow (...000)_2 \\
f_3 &= +370 \cdot 21 - 371 \cdot 11 = -74 - 159 \equiv 1728 \Rightarrow (...000)_2 \\
f_4 &= +370 \cdot 21 + 371 \cdot 11 = -74 + 159 \equiv 85 \Rightarrow (...101)_2 \quad \checkmark
\end{aligned}$$

$\Rightarrow$ The message is $m = 85$.

Solution of Problem 2

a) Since a symmetric cryptosystem is used, and since Bob knows the key k, he may compute $x = E_k^{-1}(y)$. Therefore, he knows if x is even or odd. Hence, he may always win.

b) The basic four requirements on cryptographic hash functions are:

- Given $m \in \mathcal{M}$, $h(m)$ is easy to compute.
- preimage resistant, i.e., given $y \in \mathcal{Y}$ it is infeasible to find $m \in \mathcal{M}$ such that $h(m) = y$.
- second preimage resistant, i.e., given $m \in \mathcal{M}$, it is infeasible to find $m' \neq m$ with $h(m') = h(m)$.
- (strongly) collision free, i.e., it is infeasible to find $m \neq m'$ with $h(m) = h(m')$.

c) The solution is analogous to the given protocol [E_k is exchanged by h]

1) Alice chooses a number x, calculates $y = h(x)$, and sends y to Bob
2) Bob guesses, if x is even or odd, and sends his guess to Alice
3) Alice sends x to Bob

If Bob as guessed correctly, Bob wins. Otherwise Alice wins.
[This protocol is secure since Alice cannot find another x' with $y = h(x')$, see b). Moreover, Bob cannot calculate x by means of the given y, see b).]

d) Protocol based on the factorization problem:

1) Alice chooses prime numbers p,q with $p, q \mod 4 \equiv 1$ or $p, q \mod 4 \equiv 3$.
2) Alice computes $n = pq$ ands send n to Bob
3) Bob guesses if $p, q \mod 4 \equiv 1$ or $p, q \mod 4 \equiv 3$ and sends his guess to Alice
4) A sends p, q to Bob.

If Bob has guessed correctly, Bob wins. Otherwise Alice wins.

Solution of Problem 3

a) In general, the formula $E : Y^2 = X^3 + aX + b$ with $a, b \in K$ describes an elliptic curve. Here, we have $a = 2, b = 6$ with $a, b \in \mathbb{F}_7$.
E is an elliptic curve over $\mathbb{F}_7$, since the discriminant is:

$$\Delta = -16(4a^3 + 27b^2) \equiv -16064 \equiv 1 \not\equiv 0 \pmod 7. \tag{1}$$

b) The point-counting algorithm is solved in a table:

z	z^2	z^3	$z^3 + 2z + 6$
0	0	0	6
1	1	1	2
2	4	1	4
3	2	6	4
4	2	1	1
5	4	6	1
6	1	6	3

From this table we obtain:

$$\begin{aligned} Y^2 &\in \{0, 1, 2, 4\}, \\ X^3 + 2X + 6 &\in \{0, 1, 2, 3, 4, 6\}, \end{aligned}$$

and hence it follows:

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

The inverses of each point are:

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

c) The order of the group is $\mathrm{ord}(E(\mathbb{F}_q)) = \#E(\mathbb{F}_q)) = 11$.

d) To obtain the discrete logarithm for $Q = aP$, we rearrange the equation:

$$\begin{aligned} cP + dQ &= c'P + d'Q \\ \Rightarrow (c - c')P &= (d' - d)Q = (d' - d)aP \\ &\Rightarrow a \equiv (c - c')(d' - d)^{-1} \pmod{(\mathrm{ord}(P))}. \end{aligned}$$

As $\gcd(d' - d, n) = 1$ holds, the discrete logarithm a exists.

e) The left-hand side and the right-hand side of (2) are evaluated and compared:

$$\begin{aligned}
2P &= (4,1) + (4,1) = (x_3, y_3) \\
x_3 &= ((3 \cdot 4^2 + 2)(2 \cdot 1)^{-1})^2 - 2 \cdot 4 \\
&\equiv ((3 \cdot 2 + 2)2^{-1})^2 + 6 \equiv (8 \cdot 4)^2 + 6 \equiv 1 \pmod 7 \\
y_3 &= (8 \cdot 4)(4 - 1) - 1 \equiv 4 \pmod 7 \\
\Rightarrow 2P &= (1,4)
\end{aligned}$$

For the inverse of 2 we have: $1 = 7 + 2(-3) \Rightarrow 2^{-1} \equiv 4 \pmod 7$.

$$\begin{aligned}
2P + 4Q &= (1,4) + (3,5) = (x_3, y_3) \\
x_3 &= ((5-4)(3-1)^{-1})^2 - 1 - 3 \equiv (1 \cdot 2^{-1})^2 - 4 \\
&\equiv 5 \pmod 7 \\
y_3 &= (1 \cdot 4)(1 - 5) - 4 \equiv 4(-4) - 4 \equiv 1 \pmod 7 \\
\Rightarrow 2P + 4Q &= (5,1) \\
-P - 3Q &= -(4,1) + (5,6) = (4,6) + (5,6) = (x_3, y_3) \\
x_3 &= 0 - 4 - 5 \equiv 5 \pmod 7 \\
y_3 &= 0 - 6 \equiv 1 \pmod 7 \\
\Rightarrow -P - 3Q &= (5,1)
\end{aligned}$$

Equation (2) is fulfilled. The discrete logarithm is:

$$a = (2 - (-1))((-3) - 4)^{-1} \equiv 3(-7)^{-1} \equiv 3 \cdot 3 \equiv 9 \pmod{11}$$