Dr. Michael Reyer

Tutorial 13
- Proposed Solution -

Wednesday, February 6, 2019

Solution of Problem 1

a) The Rabin cryptosystem requires $n = p\,q$ with primes $p \neq q$ and $p, q \equiv 3 \pmod 4$. As $\sqrt{989} < 32$ start with $p = 31$ which is prime and fulfills $p \equiv 3 \pmod 4$. Then $\frac{n}{p}$ is no integer. Next smaller prime with $p \equiv 3 \pmod 4$ is $p = 23$. Then for $q = 43$ it holds $n = p\,q$. Moreover, $q \equiv 3 \pmod 4$ such that all conditions are fulfilled.

b) Let $p = 7$, $q = 23$, $n = p\,q$, $c = 116$. Following Prop 9.3 it holds.

$$k_p = \frac{p+1}{4} = 2 \quad k_q = \frac{q+1}{4} = 6$$

$$x_{p,1} = c^{k_p} = 116^2 \equiv 2 \pmod 7$$
$$x_{p,2} = -x_{p,1} = -2 \equiv 5 \pmod 7$$
$$x_{q,1} = c^{k_q} = 116^6 \equiv 1 \pmod{23}$$
$$x_{q,2} = -x_{q,1} = -1 \equiv 22 \pmod{23}$$

Following Prop. 9.4 you apply the Extended Euclidean Algorithm and get:

a_n	b_n	f_n	r_n	c_n	d_n
			23	1	0
			7	0	1
23	7	3	2	1	-3
7	2	3	1	-3	10

$$\gcd(p, q) = s \cdot p + t \cdot q = 10 \cdot 7 + (-3) \cdot 23 = 1.$$

Compute the resulting square root modulo n.

$$a \equiv tq \equiv -3 \cdot 23 \equiv -69 \equiv 92 \pmod{161}$$

$$b \equiv sp \equiv 10 \cdot 7 \equiv 70 \pmod{161}$$

We obtain the four different messages as $f_{i,j} = a \cdot x_{p,i} + b \cdot x_{q,j} \mod 161$.

$$f_{1,1} \equiv 92 \cdot 2 + 70 \cdot 1 \equiv 254 \equiv 93 \pmod{161} \tag{1}$$

$$f_{1,2} \equiv 92 \cdot 2 + 70 \cdot 22 \equiv 1724 \equiv 114 \pmod{161} \tag{2}$$

$$f_{2,1} \equiv 92 \cdot 5 + 70 \cdot 1 \equiv 530 \equiv 47 \pmod{161} \tag{3}$$

$$f_{2,2} \equiv 92 \cdot 5 + 70 \cdot 22 \equiv 2000 \equiv 68 \pmod{161} \tag{4}$$

Finally, we transform the obtained values into binary notation.

$$(1)\;\; 93 = \ldots 1101_2$$

$$(2)\;\; 114 = \ldots 0010_2$$

$$(3)\;\; 47 = \ldots 1111_2 \quad \checkmark$$

$$(4)\;\; 68 = \ldots 0100_2$$

The message is $m = 47$.

c) Oscar chooses m at random and computes $c = m^2 \mod n$.
c is deciphered with plaintext m'.
With probability $\frac{1}{2}$ is $m' \neq \pm m$. In this case compute $\gcd(m - m', n) \in \{p, q\}$. Otherwise, repeat the previous steps.

d) In this case the solution of the Rabin cryptosystem can be obtained computing the square roots in the real domain. This vulnerability can be solved by padding and/or allowing messages bigger than $\sqrt{n}$ only.

Solution of Problem 2

a)
- Easy to compute,
- Preimage resistant, i.e., given y it is infeasible to find m s.t. $h(m) = y$.
- 2nd preimage resistant, i.e., given m it is infeasible to find m' s.t. $h(m) = h(m')$.
- Collision-free, i.e., it is infeasible to find $m \neq m'$ s.t. $h(m) = h(m')$.

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

c) Verification

1) Obtain the authentic public key $(v_1, v_2, ..., v_t)$.
2) Steps 2) to 4) are identical to the signature generation procedure 1) to 3) above.
5) Accept the signature if and only if $v_{i_j} = h(s_j)$ for all $1 \leq j \leq u$ holds.

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: $(k_2, k_4, k_7, k_8) = (36, 24, 9, 34)$.

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

a) Show that a is a primitive element modulo p

$$a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p},\ \forall i = 1, \ldots, k,$$

with the prime factorization $p - 1 = \prod_{i=1}^{k} p_i^{t_i} \Rightarrow a$ is a primitive element modulo p_i prime.
In this case, $112 = 2^4 \cdot 7$ and hence,

$3^{\frac{112}{7}} \equiv 49 \not\equiv 1 \pmod{113}$

$3^{\frac{112}{2}} \equiv 112 \not\equiv 1 \pmod{113}$

b) $s = k^{-1}(h(m) - xr) \mod p - 1$
$r = a^k \mod p \Rightarrow 3^{19} \equiv 80 \pmod{113}$ by SQM then

$s \equiv 59(77 - 66 \cdot 80) \equiv 15 \pmod{112}$

c) $v_1 \equiv y^r \cdot r^s \equiv y^r \cdot (a^u \cdot y^v)^s \equiv y^r \cdot a^{us} \cdot y^{vs} \equiv y^{r+vs} \cdot a^{us} \equiv 1 \cdot a^{us} \pmod{p}$ $v_2 \equiv a^m \equiv a^{us} \pmod{p}$

d) $\hat{r} = a^k \mod p$

$\hat{s} = k^{-1}(\hat{h} - x\hat{r}) \mod p - 1$

It holds $v_1 \equiv y^{\hat{r}} \hat{r}^{\hat{s}} \equiv a^{\hat{h}} \equiv v_2 \pmod{p}$

$r' = \hat{r}(h'\hat{h}^{-1}p - p + 1) \mod p(p-1)$
$s' = \hat{s}h'\hat{h}^{-1} \mod p - 1$

$s' \equiv k^{-1}(\hat{h} - x\hat{r}) \cdot h'\hat{h}^{-1} \equiv k^{-1}(h' - x\hat{r}h'\hat{h}^{-1})) \pmod{p-1}$

It should be

$r' \equiv \hat{r} \pmod{p}$
$r' \equiv \hat{r}h'\hat{h}^{-1} \pmod{p-1}$ by Chinese Remainder Theorem it holds.

$M = p(p-1)$, $M_1 = p - 1$, $M_2 = p$
$y_1 \equiv (p-1)^{-1} \equiv -1 \pmod{p}$
$y_2 \equiv p^{-1} \equiv 1 \pmod{p-1} \Rightarrow$

$\Rightarrow r' = \hat{r}(p-1)(-1) + \hat{r}h'\hat{h}^{-1} \cdot p \cdot 1 \mod p(p-1)$

e) It holds $r' > p - 1$ with high probability.

Solution of Problem 4

a) It must hold the following:

$$Y_m^2 \equiv X_m^3 + a \cdot X_m \pmod{p}.$$

Let g be a generator of $\mathbb{F}_p$, then it exists $i \in \mathbb{F}_p$, s. t. $g^i \equiv m^3 + a \cdot m \pmod{p}$. There are two different possibilities:

- If i is even, ✓.
- If i is odd, then

  $$(p-m)^3 - a(p-m) \equiv -m^3 - a \cdot m \equiv -g^i \equiv (-1) \cdot g^i \equiv g^{\frac{p-1}{2}} g^i \equiv g^{i+\frac{p-1}{2}} \pmod{p}.$$

  As i and $\frac{p-1}{2}$ are odd, as $p \equiv 3 \pmod{4}$, the sum $i + \frac{p-1}{2}$ is even. This means $y = g^{\frac{i}{2}+\frac{p-1}{4}} \bmod p$. Note that $-1 \equiv g^{\frac{p-1}{2}} \pmod{p}$ as g is generator and $\mathbb{F}_p$ is a field.

b) Let $m = x = 6$.
$y^2 = x^3 + a\,x = 6^3 + 1 \cdot 6 = 222 \equiv 91 \pmod{131}$
$2^{114} \equiv 91 \pmod{131} \Rightarrow 2^{57} \equiv y \pmod{131} \Rightarrow y = 22$

$2^4 \equiv 16 \pmod{131}$
$2^8 \equiv 125 \pmod{131}$
$2^{16} \equiv 36 \pmod{131}$
$2^{32} \equiv 117 \pmod{131}$
$2^{57} \equiv 2^{32} \cdot 2^{16} \cdot 2^8 \cdot 2^1 \equiv 22 \pmod{131}$

$22^2 \equiv 91 \pmod{131}$
It holds that $(6, 22)$ is the corresponding point on the EC.

c) For an EC it must hold $\Delta = -16(4a^3 + 27b^2) \not\equiv 0 \pmod{p}$. With $b = 0$ it holds.
$\Delta \equiv -64\,a^3 \equiv -a^3 \not\equiv 0 \pmod{7}$.
This is true for $1 \leq a \leq 6$.

d) Inserting the point $(3, 2)$ into the Elliptic curve equation:
$4 = 27 + 3a \iff 5 \equiv 3a \pmod{7} \iff a = 4$.

e) We create the following table.

x	x^2	x^3	x^3+x
0	0	0	0
1	1	1	2
2	4	1	3
3	2	6	2
4	2	1	5
5	4	6	4
6	1	6	5

Considering $y^2 \equiv x^3 + x \pmod 7$ leads to
$E_1(\mathbb{F}_7) = \{(0,0); (1,3); (1,4); (3,3); (3,4); (5,2); (5,5); \mathcal{O}\}$.

f) It holds $|E_1(\mathbb{F}_7)| = 8 = p + 1 - t \Rightarrow t = 0$. This means the order is 8 and the trace is $t = 0$.

g) As $| < P > | \mid |E_1(\mathbb{F}_7)|$ it holds that $| < P > | \in \{1, 2, 4, 8\}$.
$| < P > | \neq 1$ as $P = (3,3) \neq \mathcal{O}$
$| < P > | \neq 2$ as $2P = (1,4) \neq \mathcal{O}$
$| < P > | \neq 4$ as $4P = (1,4) + (1,4) \neq \mathcal{O}$ as $(1,4) \neq -(1,4) = (1,3)$.
Hence, $| < P > | = 8$, i.e., P is generator. Moreover $4P + 4P = \mathcal{O}$, i.e., $4P = (0,0)$ the only self-inverse point on the EC. It holds:

$$\begin{aligned} P &= (3,3) \\ 2P &= (1,4) \\ 4P = -4P &= (0,0) \\ 6P = -2P &= (1,3) \\ 7P = -P &= (3,5) \\ 8P &= \mathcal{O}. \end{aligned}$$