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

Tutorial 4
- Proposed Solution -

Friday, November 20, 2015

Solution of Problem 1

$$n = p \cdot q = 31 \cdot 79 = 2449$$

a) Apply Algorithm 7 *(Finding pseudo-squares modulo $n = pq$).*

1. $a = 10 \to \left(\frac{a}{p}\right) = 1$
   $a = 11 \to \left(\frac{a}{p}\right) = -1$ ✓
2. $b = 17 \to \left(\frac{b}{q}\right) = -1$ ✓
3. Compute $y \in \{0, 1, \ldots, n-1\}$ with

$$y \equiv a \mod p\,,$$
$$y \equiv b \mod q\,,$$

by applying the Chinese remainder theorem to solve the system of congruences.

$$m_1 = p,\ \ m_2 = q,\ \ a_1 = a,\ \ a_2 = b,\ \ x = y,$$
$$M = m_1 \cdot m_2 = n = p \cdot q,\ \ M_1 = m_2 = q,\ \ M_2 = m_1 = p,$$
$$y_1 = M_1^{-1} = q^{-1} = 11 \mod m_1,\ \ y_2 = M_2^{-1} = p^{-1} = 51 \mod m_2,$$
$$\Rightarrow y = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 = a \cdot q \cdot 11 + b \cdot p \cdot 51$$
$$= 11 \cdot 79 \cdot 11 + 17 \cdot 31 \cdot 51 \equiv 2150 \mod n$$

b)

$$\left(\frac{1418}{31}\right) = -1 \quad \Rightarrow m_1 = 1$$
$$\left(\frac{2150}{31}\right) = -1 \quad \Rightarrow m_2 = 1$$
$$\left(\frac{2153}{31}\right) = 1 \quad \Rightarrow m_3 = 0$$

$$\Rightarrow m = (1, 1, 0)$$

Solution of Problem 2

Let $p = 31$, $q = 43$. As described in the script, the initial value x_0 of the Blum-Blum-Shub generator is computed from x_{t+1}.

$$\begin{aligned} d_1 &= \left(\frac{p+1}{4}\right)^{t+1} = 8^{10} \equiv 4 \mod (p-1) \\ d_2 &= \left(\frac{q+1}{4}\right)^{t+1} = 11^{10} \equiv 25 \mod (q-1) \\ u &= x_{t+1}^{d_1} \equiv 1306^4 \equiv 8 \mod p \\ v &= x_{t+1}^{d_2} \equiv 1306^{25} \equiv 4 \mod q \end{aligned}$$

Compute the inverse $ap + bq = 1$ using the Extended Euclidean algorithm.

$$\begin{aligned} 43 &= 31 \cdot 1 + 12 \\ 31 &= 12 \cdot 2 + 7 \\ 12 &= 7 \cdot 1 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + \underline{1} \\ 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (12 - 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 \\ &= 3 \cdot 12 - 5 \cdot (31 - 12 \cdot 2) = 13 \cdot 12 - 5 \cdot 31 \\ &= 13 \cdot (43 - 31 \cdot 1) - 5 \cdot 31 \\ &= \underbrace{13}_{b} \cdot \underbrace{43}_{q} \underbrace{-18}_{a} \cdot \underbrace{31}_{p} \end{aligned}$$

We can calculate x_0 as:

$$\begin{aligned} x_0 &= (vap + ubq) \mod n \\ &\equiv 4 \cdot (-18) \cdot 31 + 8 \cdot 13 \cdot 43 \\ &\equiv -2232 + 4472 \\ &\equiv 2240 \equiv 907 \mod 1333 \end{aligned}$$

Compute $x_1, \ldots, x_9$ with $x_{i+1} = x_i^2 \mod n$.

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
907	188	686	47	876	901	4	16	256	219

Use the last five digits of the binary representation of x_i for b_i. E.g., $x_1 = 188_{10} = 10111100_2 \Rightarrow b_1 = 11100$. With $m_i = c_i \oplus b_i$, $1 \leq i \leq 9$, we can decipher the cryptogram.

i	1	2	3	4	5	6	7	8	9
c_i	10101	01110	00011	01000	10111	00101	11110	01101	11000
b_i	11100	01110	01111	01100	00101	00100	10000	00000	11011
m_i	01001	00000	01100	00100	10010	00001	01110	01101	00011
	J	A	M	E	S	B	O	N	D

Solution of Problem 3

- In a Blum-Goldwasser cryptosystem: $n = p \cdot q$, $p \neq q$, $p, q \equiv 3 \mod 4$.
- Given an arbitrary ciphertext $(c_1, \ldots, c_t, x_{t+1})$, the decoding hardware provides $(m_1, \cdots, m_t)$ but not x_0.
- We know that $b_i = m_i \oplus c_i$, $1 \leq i \leq t$.
- By assumption, we have a function $f(b_i) = x_i$, where $1 \leq i \leq t$, b_i are the last h bits of x_i, and x_i is the quadratic residue modulo n.
- We obtain a chain of consecutive squares and their respective quadratic residues.

$$x_t^2 = x_{t+1}, \ \ x_{t-1}^2 = x_t, \ \ \ldots, \ \ x_0^2 = x_1$$

- The attacker selects a random $r \in \mathbb{Z}_n^*$ and deciphers $x'_{t+1} = r^2 \mod n$.
- With positive probability $x'_t \not\equiv \pm r \mod n$. If $x'_t \equiv \pm r \mod n$, then repeat the last step.
- Using Proposition 6.8 of the lecture notes, compute

$$\gcd\left(x'_t - r, n\right) \in \{p, q\}\,.$$

  This factors n.