Dr. Michael Reyer

Tutorial 1
- Proposed Solution -

Friday, October 26, 2018

Solution of Problem 1

Decipher $m = \sqrt{c} \mod n$ with $c = 1935$.

- Check $p, q \equiv 3 \pmod 4$ ✓
- Compute the square roots of c modulo p and c modulo q.

$$\begin{aligned}
&k_p = \frac{p+1}{4} = 17, \quad k_q = \frac{q+1}{4} = 18,\\
&x_{p,1} = c^{k_p} \equiv 1935^{17} \equiv 59^{17} \equiv 40 \pmod{67},\\
&x_{p,2} = -x_{p,1} \equiv 27 \pmod{67},\\
&x_{q,1} = c^{k_q} \equiv 1935^{18} \equiv 18^{18} \equiv 36 \pmod{71},\\
&x_{q,2} = -x_{q,1} \equiv 35 \pmod{71}.
\end{aligned}$$

- Compute the resulting square root modulo n. $m_{i,j} = ax_{p,i} + bx_{q,j}$ solves $m_{i,j}^2 \equiv c \pmod n$ for $i, j \in \{1, 2\}$. We substitute $a = tq$ and $b = sp$. Then $tq + sp = 1$ yields $1 = 17 \cdot 71 + (-18) \cdot 67 = tq + sp$ from the Extended Euclidean Algorithm.

$$\begin{aligned}
&\Rightarrow a \equiv tq \equiv 17 \cdot 71 \equiv 1207 \pmod n\\
&\Rightarrow b \equiv sp \equiv -18 \cdot 67 \equiv -1206 \pmod n.
\end{aligned}$$

  The four possible solutions for the square root of ciphertext c modulo n are:

$$\begin{aligned}
m_{1,1} &\equiv ax_{p,1} + bx_{q,1} \equiv 107 \pmod n \Rightarrow 00000011010\underline{11},\\
m_{1,2} &\equiv ax_{p,1} + bx_{q,2} \equiv 1313 \pmod n \Rightarrow 0010100100001,\\
m_{2,1} &\equiv ax_{p,2} + bx_{q,1} \equiv 3444 \pmod n \Rightarrow 0110101110100,\\
m_{2,2} &\equiv ax_{p,2} + bx_{q,2} \equiv 4650 \pmod n \Rightarrow 1001000101010.
\end{aligned}$$

  The correct solution is m_1, by the agreement given in the exercise.

Solution of Problem 2

a) Given $x \equiv -x \pmod p$, prove that $x \equiv 0 \pmod p$.

Proof. The inverse of 2 modulo p exists. Then,

$$\begin{aligned} -x &\equiv x \pmod{p} \\ \Leftrightarrow \quad 0 &\equiv 2x \pmod{p} \\ \Leftrightarrow \quad 0 &\equiv x \pmod{p}\,. \end{aligned}$$

□

b) Assume $x^2 \equiv y^2 \pmod{p^2}$ and $x \not\equiv \pm y \pmod{p^2}$ then Prop. 6.8 ($n = p^2$) tells that $\gcd(x-y, p^2)$ yields a non-trivial factor of p^2. In our case it is p. Moreover, $(x-y)(x+y) \equiv 0 \pmod{p^2}$ it follows that $p \mid (x-y)$ and $p \mid (x+y)$, i.e. it exists $k, l \in \mathbb{N}$ s.t. $x - y = kp$ and $x + y = lp$. Adding up leads to $2x = (k+l)p$, i.e. $p \mid x$ which is a contradiction to $x \not\equiv 0 \pmod{p}$.

c) $p = 7$, $p^2 = 49$, $c = 37$. Then

$$\begin{aligned} b = c^{\frac{p+1}{4}} = 37^{\frac{7+1}{4}} = 37^2 \equiv 4 &\pmod{p}\,, \\ b^{-1} \equiv 2 \pmod{p}\,,\ 2^{-1} \equiv 4 &\pmod{p}\,, \\ a = \frac{c - b^2}{p} \cdot 2^{-1} \cdot b^{-1} = \frac{37 - 4^2}{7} \cdot 4 \cdot 2 \equiv 3 &\pmod{p} \\ x = b + ap = 4 + 3 \cdot 7 = 25 & \end{aligned}$$

Check: $x^2 = 25^2 \equiv 37 = c \pmod{p^2}$.
Remark: That this procedure is valid can be deduced by Hensels Lemma.

d) Bob just needs to calculate the square root of n in the reals. Thereby, he can discover the cheat and win, as he can factorize n. However, by sending the factors he should recognize that there are no two distinct prime numbers chosen.

e) Looking at the protocol, we can show that Bob almost always loses to Alice, if she chooses $p = q$.

i) Alice calculates $n = p^2$ and sends n to Bob.

ii) Bob calculates $c \equiv x^2 \mod n$ and sends c to Alice. If $p \mid x$ then $c = 0$ which should not be possible. Then Bob should get suspicious. This happens with low probability.

iii) The only two solutions $\pm x$ are calculated by Alice and sent to Bob. Bob cannot factor n, as

$$\gcd(x - (\pm x), n) = \begin{cases} \gcd(0, n) = n \\ \gcd(2x, n) = \gcd(2x, p^2) = 1 \end{cases}.$$

Alice always wins.