Exercise 1 in Advanced Methods of Cryptography
- Proposed Solution -

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

2014-10-24

Solution of Problem 1

"⇒" c is QR modulo p with Definition 9.1 it follows

$$\exists\, x \in \mathbb{Z}_p^* : x^2 \equiv c \mod p \Rightarrow c^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p,$$

where the last congruence follows from Fermat's Theorem.

"⇐" $c^{\frac{p-1}{2}} \equiv 1 \mod p \Rightarrow c \in \mathbb{Z}_p^*$ as c has an inverse modulo p.
Let y be a primitive element (PE), i.e., y is a generator of $\mathbb{Z}_p^*$. Note that there exists a primitive element with respect to Theorem 7.2 a).

$$\begin{aligned}
&\Rightarrow \quad \exists\, j : c \equiv y^j \mod p \\
&\Rightarrow \quad c^{\frac{p-1}{2}} \equiv (y^j)^{\frac{p-1}{2}} \equiv 1 \mod p \\
&\Rightarrow \quad p-1 \mid j(p-1)/2 \Rightarrow j \text{ must be even} \\
&\Rightarrow \quad \exists\, x \in \mathbb{Z}_p^* : x \equiv y^{\frac{j}{2}} \mod p \\
&\Rightarrow \quad x^2 \equiv y^j \equiv c \mod p \\
&\Rightarrow \quad c \text{ is QR modulo } p
\end{aligned}$$

Solution of Problem 2

a) Show that the Babystep-Giantstep-Algorithm computes the discrete logarithm.

$$\begin{aligned}
b_j &= \alpha^j \mod p, \\
g_i &= \beta\alpha^{-im} \mod p, \\
x &\equiv j + im \mod p-1
\end{aligned}$$

The equation $b_j \equiv g_i$ yields:

$$\begin{aligned}
\alpha^j &\equiv \beta\alpha^{-im} \mod p \\
\alpha^{j+im} &\equiv \beta \mod p \\
\alpha^x &\equiv \beta \mod p
\end{aligned}$$

b) a being a primitive element of the group $\mathbb{Z}_p^*$ means, all elements in the group $\beta \in \mathbb{Z}_p^*$ have a representation as $a^n \mod p, n \in \{0, \ldots, p-1\}$. This guarantees existence and uniqueness in the output of the algorithm.

Take for example $a = 1$, which is obviously no primitive element. Then, $b_j = 1 \, \forall j$ and $g_i = \beta \, \forall i$. No value $\beta \neq 1$ has a solution for n. $\beta = 1$ is the only possible value, but the solution for n is not unique.

c) $\alpha^x \equiv \beta \mod p$, $\alpha = 3$, $p = 29$, $\beta = 13$.

Task: Compute $x = \log_\alpha(\beta)$ using the Babystep-Giantstep-Algorithm.

(1) $m = \lceil 29 \rceil = 6$

i/j	0	1	2	3	4	5
(2) $b_j = \alpha^j \mod p$	1	3	9	27	23	11
(3) $g_i = \beta\alpha^{-im} \mod p$	13	25	28	7	9	24

Note that $\alpha^{-1} \equiv 10 \mod p$, since $3 \cdot 10 - 1 \cdot 29 = 1 \Rightarrow \alpha^{-m} \equiv 10^6 \equiv 22 \mod 29$.

(4) For $(j, i) = (2, 4) \Rightarrow b_2 = g_4 = 9$ holds

$$\begin{aligned} x &= mi + j \mod (p-1) \\ &\equiv 6 \cdot 4 + 2 \mod 28 \\ &\equiv 26 \mod 28 \end{aligned}$$

The discrete logarithm is $x = 26$.
(Check: $3^{26} = 3^{13}3^{13} \equiv 19 \cdot 19 \equiv 13 \mod 29$)

Remark on complexity:

Running: $2\sqrt{p} \approx \mathcal{O}(\sqrt{p})$

Bruteforce: $\mathcal{O}(p)$

Solution of Problem 3

It is to prove that

$$a^x \equiv a^y \mod n \Leftrightarrow x \equiv y \mod \operatorname{ord}_n(a)$$

with $x, y \in \mathbb{Z}$, $a \in \mathbb{Z}_n^*$, $a \neq 1$, and $\operatorname{ord}_n(a) = k$.

"$\Rightarrow$ Let $a^x \equiv a^y \mod n \Rightarrow a^{x-y} \equiv 1 \mod n$ and $a^k \equiv 1 \mod n \Rightarrow \operatorname{ord}_n(a) = k$.
Recall: $\operatorname{ord}_n(a) = \min\{k \in \{1, \ldots, \varphi(n) \mid a^k \equiv 1 \mod n\}\}$.

$$\begin{aligned} & k \mid (x-y) \\ \Rightarrow\ & x \equiv y \mod k \\ \Rightarrow\ & x \equiv y \mod \operatorname{ord}_n(a). \end{aligned}$$

"$\Leftarrow$ Let $x \equiv y \mod \operatorname{ord}_n(a) \Rightarrow k \mid (x-y) \Rightarrow x - y = kl, l \in \mathbb{Z}$.

$$\begin{aligned} &\Rightarrow a^{x-y} \equiv a^{kl} \equiv (a^k)^l \equiv 1^l \equiv 1 \mod n \\ &\Rightarrow a^{x-y} \equiv 1 \mod n \Rightarrow a^x \equiv a^y \mod n. \end{aligned}$$