Chair for Theoretical Information Technology
RWTH AACHEN UNIVERSITY

Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 10
- Proposed Solution -

Friday, July 1, 2016

Solution of Problem 1

Proof. "⇒" If a is a primitive element modulo p, then, by definition, $\text{ord}_p(a) = p-1$. Since $\frac{p-1}{p_i} < p-1 = \text{ord}_p(a)$,

$$\forall i : a^{\frac{p-1}{p_i}} \not\equiv 1 \mod p\,.$$

"⇐" If a is *not* a primitive Element modulo p, then $\text{ord}_p(a) = k$ and $k|(p-1)$. Then

$$\exists c \neq 1 \text{ with } p-1 = k \cdot c\,.$$

Since $c \neq 1$, it holds that $p_i|c$ for some i. For that i, we get

$$a^{\frac{p-1}{p_i}} \equiv a^{\frac{k\cdot c}{p_i}} \equiv \underbrace{(a^k)}_{\equiv 1, \text{ since } k=\text{ord}_p(a)}{}^{\frac{c}{p_i}} \equiv 1 \mod p\,.$$

□

Solution of Problem 2

This problem is usually a difficult problem, but we can solve it, because 31 is prime. First, apply Proposition 7.5 to show that 17 is a primitive element modulo 31.

$$\begin{aligned}
17^{\frac{p-1}{p_i}} &\overset{!}{\not\equiv} 1 \mod p \quad \forall i = 1,\dots,k, \quad \text{where } p-1 = \textstyle\prod_{i=1}^{k} p_i^{t_i}\\
p = 31 &\Rightarrow p-1 = 30 = 2\cdot 3\cdot 5\\
17^{\frac{30}{2}} &\equiv 30 \not\equiv 1 \mod 31\\
17^{\frac{30}{3}} &\equiv 25 \not\equiv 1 \mod 31\\
17^{\frac{30}{5}} &\equiv 8 \not\equiv 1 \mod 31
\end{aligned}$$

17 is a primitive element modulo 31 and we can conclude:

$$\begin{aligned}
\exists b : 17^b &\equiv a \mod 31\\
(a^{13})^b &\equiv a \mod 31\\
a^{13\cdot b-1} &\equiv 1 \mod 31
\end{aligned}$$

With Fermats little theorem (Theorem 6.2, let $a \in \mathbb{Z}_n^*$, then $a^{\varphi(n)} \equiv 1 \mod n$), we can say:

$$\begin{aligned} a^{\varphi(n)} &\equiv a^{30} \equiv 1 \mod 31 \\ a^{13\cdot b-1} &\equiv a^{30} \equiv 1 \mod 31 \\ \Rightarrow 13 \cdot b - 1 &\equiv 30 \mod 30 \\ 13 \cdot b &\equiv 1 \mod 30 \\ b &\equiv 13^{-1} \mod 30 \end{aligned}$$

The Extended Euclidean Algorithm yields $13 \cdot 7 - 30 \cdot 3 = 1$ and thus $b = 13^{-1} \equiv 7 \mod 30$. It remains to compute $a \equiv 17^b \equiv 17^7 \equiv 12 \mod 31$.

Solution of Problem 3

Public parameters: $a = 2$, $p = 107$

Secret parameters: $x_A = 66$ and $x_B = 33$

a) First encrypted exponent A $\rightarrow$ B:

$$\begin{aligned} u &= a^{x_A} \mod p \\ &= 2^{66} \mod 107 \\ &= (2^{10})^6 \cdot 2^6 \equiv (61 \cdot 2)^6 \equiv 15^6 \\ &\equiv 11\,390\,625 \equiv 47 \mod 107 \end{aligned}$$

Second encrypted exponent B $\rightarrow$ A:

$$\begin{aligned} v &= a^{x_B} \mod p \\ &= 2^{33} \mod p \\ &= (61 \cdot 2)^3 \equiv 15^3 \equiv 58 \mod 107 \end{aligned}$$

A computes the shared key with: $v^{x_A} = 58^{66} \mod 107$. We use the *square and multiply* algorithm to compute the exponentiation. First, we compute the binary representation of 66:

$$\begin{aligned} 66 &= 2 \cdot 33 + 0 \\ 33 &= 2 \cdot 16 + 1 \\ 16 &= 2 \cdot 8 + 0 \\ 8 &= 2 \cdot 4 + 0 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 2 \cdot 1 + 0 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

The binary representation of 66 is $66_{10} = 1000010_2$.

A computes the shared key by:

$$\begin{aligned} 58^2 &= 3364 \equiv 47 \mod 107 \\ 47^2 &= 2209 \equiv 69 \mod 107 \\ 69^2 &= 4761 \equiv 53 \mod 107 \\ 53^2 &= 2809 \equiv 27 \mod 107 \\ 27^2 \cdot 58 &= 42\,282 \equiv 17 \mod 107 \\ 17^2 &= 289 \equiv 75 \mod 107 \end{aligned}$$

B computes the shared key by: $u^{x_B} = 47^{33} \mod 107$, with $33_{10} = 100001_2$.

$$\begin{aligned} 47^2 &= 2209 \equiv 69 \mod 107 \\ 69^2 &= 4761 \equiv 53 \mod 107 \\ 53^2 &= 2809 \equiv 27 \mod 107 \\ 27^2 &= 729 \equiv 87 \mod 107 \\ 87^2 \cdot 47 &= 355\,743 \equiv 75 \mod 107 \end{aligned}$$

75 is the shared key of A and B.

b) With Proposition 7.5,

$$p-1 = \prod_{i=1}^{k} p_i^{t_i} \Rightarrow 107-1 = 106 = \underbrace{53}_{p_1} \cdot \underbrace{2}_{p_2}, \quad t_1 = t_2 = 1$$

$$\forall i : b^{\frac{p-1}{p_i}} \not\equiv 1 \mod p \Leftrightarrow b \text{ is a primitive element modulo } p$$
$$i = 1 : 103^2 \equiv 16 \not\equiv 1 \mod 107$$
$$i = 2 : 103^{53} \equiv 106 \not\equiv 1 \mod 107$$

The last step is computed using $53_{10} = 110101_2$:

$$\begin{aligned} 103^2 \cdot 103 &= 1\,092\,727 \equiv 43 \mod 107 \\ 43^2 &= 1849 \equiv 30 \mod 107 \\ 30^2 \cdot 103 &= 92\,700 \equiv 38 \mod 107 \\ 38^2 &= 1444 \equiv 53 \mod 107 \\ 53^2 \cdot 103 &= 289\,327 \equiv 106 \mod 107 \end{aligned}$$

As a result, $b = 103$ is a primitive element mod p.

Solution of Problem 4

Let $n = p \cdot q$, $p \neq q$ be prime and x a non-trivial solution of $x^2 \equiv 1$ $(mod\ n)$, i.e., $x \not\equiv \pm 1\ (mod\ n)$. Then:

$$\gcd(x+1, n) \in \{p, q\}$$

Proof:

$$\begin{aligned} x^2 \equiv 1\ (mod\ n) &\iff (x^2-1) \equiv 0\ (mod\ n) \\ &\iff (x+1)(x-1) \equiv 0\ (mod\ n) \\ &\iff (x+1)(x-1) = k \cdot p \cdot q \quad \exists k \in \mathbb{N} \end{aligned}$$

$$\begin{aligned} &\iff p \cdot q \mid (x+1)(x-1) \\ &\iff p \text{ divides either } (x+1) \text{ or } (x-1) \\ &\iff q \text{ divides either } (x+1) \text{ or } (x-1) \end{aligned}$$

and $x-1 < x+1 < n$ holds:

$$\iff p \cdot q \nmid (x+1) \iff p \cdot q > x+1$$

$$\Longrightarrow gcd(x+1,n) \neq p \cdot q = n$$

$$\Longleftrightarrow p \cdot q \nmid (x-1) \Longleftrightarrow p \cdot q > x-1$$

$\Longleftrightarrow$ either p or q divide $x+1 \Longrightarrow \gcd(x+1,n) \in \{p,q\}$ ✓