Exercise 9 in Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo
2015-07-02

Solution of Problem 28

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: $\operatorname{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n) \mid a^k \equiv 1 \mod n\}\}$.
$$\begin{aligned} & k \mid (x-y) \\ \Rightarrow\ & x \equiv y \mod k \\ \Rightarrow\ & x \equiv y \mod \operatorname{ord}_n(a). \end{aligned}$$

"$\Leftarrow$" Let $x \equiv y \mod \operatorname{ord}_n(a) \Rightarrow k \mid (x-y) \Rightarrow x - y = kl, l \in \mathbb{Z}$.
$$\begin{aligned} & \Rightarrow a^{x-y} \equiv a^{kl} \equiv (a^k)^l \equiv 1^l \equiv 1 \mod n \\ & \Rightarrow a^{x-y} \equiv 1 \mod n \Rightarrow a^x \equiv a^y \mod n. \quad \square \end{aligned}$$

Solution of Problem 29

Proof. "$\Rightarrow$" If a is a primitive element modulo p, then, by definition, $\operatorname{ord}_p(a) = p - 1$. Since $\frac{p-1}{p_i} < p - 1 = \operatorname{ord}_p(a)$,
$$\forall i : a^{\frac{p-1}{p_i}} \not\equiv 1 \mod p\,.$$
"$\Leftarrow$" If a is *not* a primitive Element modulo p, then $\operatorname{ord}_p(a) = k$ 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
$$a^{\frac{p-1}{p_i}} \equiv a^{\frac{k \cdot c}{p_i}} \equiv \underbrace{(a^k)}_{\equiv 1,\text{ since } k = \operatorname{ord}_p(a)}{}^{\frac{c}{p_i}} \equiv 1 \mod p\,.$$
$\square$

Solution of Problem 30

Let a be a primitive element modulo n, i.e., $\mathbb{Z}_n^* = \{a^1, a^2, \ldots, a^{\varphi(n)} \equiv 1 \equiv a^0\}$.
Let $j \in \{1, \ldots, \varphi(n)-1\}$ and $b = a^j \pmod{n}$. Then,

$$\begin{aligned}
&b \text{ is a primitive element modulo } n\\
\Leftrightarrow\ & b^k \not\equiv 1 \,(\operatorname{mod} n),\ \forall k = 1, \ldots, \varphi(n)-1 \ \wedge\ b^{\varphi(n)} \equiv 1 \,(\operatorname{mod} n)\\
\Leftrightarrow\ & a^{jk} \not\equiv 1 \,(\operatorname{mod} n),\ \forall k = 1, \ldots, \varphi(n)-1 \ \wedge\ a^{j\varphi(n)} \equiv 1 \,(\operatorname{mod} n)\\
\Rightarrow\ & a^{jk} \not\equiv a^0 \,(\operatorname{mod} n)\\
\Leftrightarrow\ & jk \not\equiv 0 \,(\operatorname{mod} \varphi(n)) \qquad (1)\\
\Leftrightarrow\ & \gcd(j, \varphi(n)) = 1. \qquad (2)
\end{aligned}$$

Proof of (2):

"$\Rightarrow$" Assume $\gcd(j, \varphi(n)) = c > 1$:

$$\underbrace{\left(\frac{\varphi(n)}{c}\right)}_{\in \{1,\ldots,\varphi(n)-1\}} \cdot j \equiv \varphi(n) \cdot \frac{j}{c} \equiv 0 \,(\operatorname{mod} \varphi(n)),$$

but $jk \not\equiv 0 \,(\operatorname{mod} \varphi(n))$, $\forall k \in \{1, \ldots, \varphi(n)-1\}$ is a contradiction. $\lightning$

"$\Leftarrow$" Assume $\gcd(j, \varphi(n)) = 1$:

$$\begin{aligned}
&\Rightarrow j \text{ is invertible modulo } \varphi(n)\\
&\Rightarrow \exists l \in \mathbb{Z} : jl \equiv 1 \,(\operatorname{mod} \varphi(n)).
\end{aligned}$$

Assume: $jk \equiv 0 \,(\operatorname{mod} \varphi(n))$ for some $k \in \{1, \ldots, \varphi(n)-1\}$:

$$\begin{aligned}
&\Rightarrow l \cdot 0 \equiv \underbrace{l \cdot j}_{\equiv 1} \cdot k \,(\operatorname{mod} \varphi(n))\\
&\Rightarrow 0 \ \equiv k \,(\operatorname{mod} \varphi(n)),
\end{aligned}$$

But $0 \notin \{1, \ldots, \varphi(n-1)\}$ is a contradiction. $\lightning$
Thus, $jk \not\equiv 0 \,(\operatorname{mod} \varphi(n))$ is necessary.

- Altogether, a^j is a primitive element modulo $n \Leftrightarrow \gcd(j, \varphi(n)) = 1$.
- The number of primitive elements modulo n is equal to:

$$|\{j \in \{1, \ldots, \varphi(n)-1\} \mid \gcd(j, \varphi(n)) = 1\}| = \varphi(\varphi(n)). \ \square$$

Solution of Problem 31

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

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

a) First encrypted exponent A $\to$ 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 $\to$ 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.