Homework 8 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

10.01.2014

Solution to Exercise 21.

Let a be a primitive element (PE) modulo n, i.e.,

$$\mathbb{Z}_n^* = \{a^1, a^2, \dots, \underbrace{a^{\varphi(n)}}_{\equiv 1 \equiv a^0}\}.$$

There exists a PE modulo n as $\mathbb{Z}_n^*$ is cyclic. Let $j \in \{1, \dots, \varphi(n)\}$ and $b = a^j \mod n$. Then,

$$\begin{aligned}
&b \text{ is a primitive element modulo } n\\
\Leftrightarrow\ & b^k \not\equiv 1 \pmod{n},\ \forall k = 1, \dots, \varphi(n) - 1 \ \wedge\ b^{\varphi(n)} \equiv 1 \pmod{n}\\
\Leftrightarrow\ & a^{jk} \not\equiv 1 \pmod{n},\ \forall k = 1, \dots, \varphi(n) - 1 \ \wedge\ a^{j\varphi(n)} \equiv 1 \pmod{n}\\
\Rightarrow\ & a^{jk} \not\equiv a^0 \pmod{n},\ \forall k = 1, \dots, \varphi(n) - 1\\
\Leftrightarrow\ & jk \not\equiv 0 \pmod{\varphi(n)},\ \forall k = 1, \dots, \varphi(n) - 1 \text{ , cf. exercise 24}\\
\Leftrightarrow\ & \gcd(j, \varphi(n)) = 1.
\end{aligned} \tag{1}$$

Proof of (1):

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

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

but $jk \not\equiv 0 \pmod{\varphi(n)}$, $\forall k \in \{1, \dots, \varphi(n) - 1\}$ is a contradiction.

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

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

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

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

But $0 \notin \{1, \dots, \varphi(n-1)\}$ and hence this is a contradiction.

Thus, $jk \not\equiv 0 \pmod{\varphi(n)}$ 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:

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