Homework 6 in Advanced Methods of Cryptography - Proposal for Solution -

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

20.11.2012

Solution to Exercise 16.

Let $\varphi : \mathbb{N} \to \mathbb{N}$ the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$ with $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.

(a) Let $n = p$ be prime. It follows
$\mathbb{Z}_p^* = \{a \in \mathbb{Z}_p \mid \gcd(a, p) = 1\} = \{1, 2, \dots, p - 1\} \Rightarrow \varphi(p) = p - 1$.

(b) Let $n = p^k$ for a prime p and $k \in \mathbb{N}$. For $1 \leq a \leq p^k$ it holds

1) $p \nmid a \Rightarrow \gcd\left(a, p^k\right) = 1$, and
2) $p \mid a \Rightarrow \gcd\left(a, p^k\right) \geq p$.

It follows $\mathbb{Z}_{p^k}^* = \underbrace{\{1 \leq a \leq p^k\}}_{p^k \text{ elements}} \setminus \underbrace{\{1 \leq a \leq p^k \mid p \mid a\}}_{p^{k-1} \text{ elements}}$. Consequently, it holds
$\varphi\left(p^k\right) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

(c) Let $n = p\,q$ for two primes $p \neq q$. It holds

1) $p \mid a \vee q \mid a \Rightarrow \gcd(a, p\,q) > 1$, and
2) $p \nmid a \wedge q \nmid a \Rightarrow \gcd(a, p\,q) = 1$.

It follows

$$\mathbb{Z}_{p\,q}^* = \underbrace{\{1 \leq a \leq p\,q - 1\}}_{p\,q-1 \text{ elements}} \setminus \left[\underbrace{\{1 \leq a \leq p\,q - 1 \mid p \mid a\}}_{q-1 \text{ elements}} \,\dot\cup\, \underbrace{\{1 \leq a \leq p\,q - 1 \mid q \mid a\}}_{p-1 \text{ elements}}\right].$$

Consequently,
$\varphi(p\,q) = p\,q - 1 - (q - 1 - p - 1) = p\,q - p - q + 1 = (p - 1)(q - 1) = \varphi(p)\,\varphi(q)$.

(d) $\varphi(4913) = \varphi\left(17^3\right) \overset{(b)}{=} 17^2(17 - 1) = 4624$ and
$\varphi(899) = \varphi\left(30^2 - 1^2\right) = \varphi((30 - 1)(30 + 1)) = \varphi(29 \cdot 31) \overset{(c)}{=} 28 \cdot 30 = 840$.