Homework 6 in Advanced Methods of Cryptography

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

20.11.2012

Exercise 15. Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ-function, i. e., $\varphi(n) = |\mathbb{Z}_n^*|$. Now let $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$.

(a) Prove Euler's Theorem: $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Exercise 16. Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ-function, i. e., $\varphi(n) = |\mathbb{Z}_n^*|$ with $n \in \mathbb{N}$.

(a) Determine $\varphi(p)$ for a prime p.

(b) Determine $\varphi(p^k)$ for a prime p and $k \in \mathbb{N}$.

(c) Determine $\varphi(p \cdot q)$ for two different primes $p \neq q$.

(d) Determine $\varphi(4913)$ and $\varphi(899)$.

Exercise 17. We consider Wilson's primality test:

$$\text{An integer } n > 1 \text{ is prime} \Leftrightarrow (n-1)! \equiv -1 \pmod{n}.$$

(a) Prove Wilson's primality test.

(b) Check if 29 is a prime number by using the given test.

(c) Is it useful in practical applications?