Homework 6 in Cryptography

Prof. Dr. Rudolf Mathar, Markus Rothe, Milan Zivkovic

26.06.2014

Exercise 22. There are four so called *weak* DES keys. One of those is the key

$$K = 00011111\ 00011111\ 00011111\ 00011111\ 00001110\ 00001110\ 00001110\ 00001110.$$

(a) What happens if you use this key?

(b) Can you find the other three weak keys?

Exercise 23. Let $\varphi : \mathbb{N} \to \mathbb{N}$ be the Euler φ-function, i.e., $\varphi(n) = |\mathbb{Z}_n^*|$.

(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 24.

(a) Use the Miller-Rabin Primality Test to prove that 341 is composite.

(b) The Miller-Rabin Primality Test comprises a number of successive squarings. Suppose a 300-digit number n is given. How many squarings are needed in worst case during a single run of this primality test?