Exercise 8 in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-06-25

Problem 24. *(determine φ)* 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 $\varphi(899)$.

Problem 25. (*MRPT error probability*) The Miller-Rabin Primality Test (MPRT) is applied m times, with $m \in \mathbb{N}$, to check whether n is prime. The number n is chosen according to a uniform distribution on the odd numbers in $\{N, \dots, 2N\}$, $N \in \mathbb{N}$.

a) Show that

$$P(\text{"}n \text{ is composite"} \mid \text{MRPT returns } m \text{ times "}n \text{ is prime"}) \leq \frac{\ln(N) - 2}{\ln(N) - 2 + 2^{2m+1}}.$$

b) How many repetitions m are needed to ensure that the above probability stays below $1/1000$ for $N = 2^{512}$?

Hint: Assume $P(\text{"}n \text{ is prime"}) = 2/\ln(N)$.

Problem 26. (*MRPT expected number of tests*) Let $n \in \mathbb{N}$ be odd and composite. Repeat the MRPT with uniformly distributed random numbers $a \in \{2, \dots, n-1\}$ until the output is "n is composite". Assume that the probability of the test outcome "n is prime" is $\frac{1}{4}$.

a) Compute the probability, that the number of such tests is equal to M, for $M \in \mathbb{N}$.

b) What is the expected value of the number of tests?

Problem 27. *(proof Wilson's primality criterion)*

Wilson's primality criterion: An integer $n > 1$ is prime $\Leftrightarrow$ $(n-1)! \equiv -1 (\bmod n)$.

a) Prove Wilson's primality criterion.

b) Check if 29 is a prime number by using the criterion above.

c) Is this criterion useful in practical applications?