Homework 10 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

12.01.2010

Exercise 28.

a) Use Fermat's Primality Test to prove that 341 is composite.

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

Exercise 29.

a) 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?

b) Let $n \in \mathbb{N}$, odd and composite. Repeat the Miller Rabin primality test with uniformly distributed random numbers $a \in \{2, \ldots, n-1\}$ until the output is "n composite". Assume that the probablity of the test outcome "n prime" is $\frac{1}{4}$.

Compute the probability, that the number of such tests is equal to M, $M \in \mathbb{N}$. What is the expected value of the number of tests?

Exercise 30.

Compute the greatest common divisor d of 4147 and 10672 and compute x and y such that $4147x + 10672y = d$.