Homework 10 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig

14.01.2008

Exercise 28.

(a) Use the Miller-Rabin Primality Test to show 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?

Exercise 29. Let $n \in \mathbb{N}$ be odd and composite. Repeat the Miller Rabin primality test with uniformly distributed random numbers $a \in \{2, \dots, n-1\}$ until the output is "n composite". Assume, that the probability, that the output of the test is "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. Pierre de Fermat is said to have factored numbers n by decomposing them as

$$n = x^2 - y^2 = (x - y)(x + y).$$

Use this method to factor the integer $n = 13199$. Describe an algorithm to determine the above x and y. Can this method be applied in general for any n?