Homework 9 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

13.01.2009

Exercise 26. Prove Wilson's primality criterion: An integer n is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Use this to show that 31 is a prime number. Why is this criterion useless for practical applications?

Exercise 27. Let n be an integer. A very simple primality test (i.e. to check whether n is prime) is trial division by possible prime divisors p. Up to which size of a prime p do you have to do trial divisions to make sure your decision is correct? How many divisions do you have to make for a number $n \approx 10^{75}$ in worst case?

Hint: Use the prime number theorem which says that the number of primes up to size x is approximately $x/\ln x$.

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?