RWTH AACHEN UNIVERSITY — Lehrstuhl für Theoretische Informationstechnik

Homework 6 in Cryptography I

Prof. Dr. Rudolf Mathar, Paul de Kerret, Georg Bocherer

24.06.2010

Exercise 16.

a) Use Fermat's Primality Test to prove that 341 is composite.
Hint: Use the square and multiply Algorithm from Script, page 52. Alternatively, `www.wolframalpha.com` can do modulo arithmetic with large numbers.

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

Exercise 17.

a) The Miller-Rabin Primality Test comprises a number of successive squarings. How many squarings are needed in worst case during a single run of this primality test? How large is this number if n has 300 digits?

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 18. Pierre de Fermat is said to have factored numbers n by decomposing them as

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

a) Show that if n is odd then such a decomposition exists.
Hint: Assume $n = ab$ and use the "binomischen Formeln" to express x and y in terms of a and b.

b) Consider the following two strategies:

A. Assign x to its minimum value. Calculate y from Fermat's formula. Check if y is an integer. If not, increase x by one and repeat.

B. Assign y to its minimum value. Calculate x from Fermat's formula. Check if x is an integer. If not, increase y by one and repeat.

Denote by $\#(A)$ and $\#(B)$ the number of times the integer check is applied until x and y are found. Assuming $n = ab$ and using the formula from a), give formulas for $\#(A)$ and $\#(B)$ in terms of a and b.

c) Which of the strategies A and B is better?