Cryptography, winter 2014/2015

PRIV.-DOZ. DR. ADRIAN SPALKA, DR. DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until
Wednesday, 28 January 2015, 23:59:59

Exercise 11.1 (Primality Testing). (13+6 points)

In this exercise we put hands on the primality tests discussed in the lecture.

(i) Implement the Fermat test in a programming language of your choice. $\boxed{2}$

(ii) Implement the strong pseudoprimality test in a programming language of your choice. $\boxed{3}$

Now, let's run it! Execute the strong pseudoprimality test with

(iii) $N = 41, x = 2$. $\boxed{1}$

(iv) $N = 57, x = 37$. $\boxed{1}$

(v) $N = 1105, x = 47$. $\boxed{1}$

(vi) $N = 1105, x = 2$. $\boxed{1}$

With our implementation running, we can now perform several experiments.

(vii) Compute the number of Fermat liars for $N = 35$, i.e. the number of choices $x \in \mathbb{Z}_N$ for which the Fermat test returns "N is possibly prime". $\boxed{2}$

(viii) Compute the number of Strong liars for $N = 35$, i.e. the number of choices $x \in \mathbb{Z}_N$ for which the Strong primality test returns "N is probably prime". $\boxed{1}$

(ix) Do the same for $N = 561$. $\boxed{1}$

(x) Perform more experiments and interpret the results. $\boxed{+6}$

Exercise 11.2 (Find a prime). (4 points)

Find a 1024bit prime. Explain how you obtained it and why you believe that it is prime. 4

Exercise 11.3 (Key lengths). (6 points)

Study the webpage `http://www.keylength.com`. There, you find various methods of estimating the necessary key-length for secure communication for a certain year.

2 (i) Explain in your own words what this website is all about.

2 (ii) Find out which key-length for RSA is recommended for the year 2015. What about AES?

2 (iii) Give an estimate till when RSA-2048 is considered to be secure (assuming no surprising progress in its cryptanalysis). Do the same for AES-128.