TP 11: discrete logarithm and Diffie-Hellman protocol

Jean-Sébastien Coron

Université du Luxembourg

1 Generating prime p such that $(p-1)/2$ is prime

Write a function that generates a prime p such that $(p-1)/2$ is prime, for a small integer p.

Write the same function for big integers.

2 Finding a generator

Write a function that given a prime p such that $(p-1)/2$ is prime, outputs a generator of $\mathbb{Z}_p^*$, for a small integer p.

Write the same function for big integers.

3 Diffie-Hellman protocol

Implement the Diffie-Hellman protocol between Alice and Bob, using a big integer library.