Sécurité des systèmes d'information
Exercise sheet 3 : Modular arithmetic

08 Octobre 2019

Non-mandatory exercise sheet. Please upload your answers on Moodle before Monday **14/10/2019 17h15**.

All answers should be carefully justified.

Exercise 1 : Number theory

1. By hand :
   - Find all prime numbers ≤ 50. Are 233 and 254 relatively prime ?
   - Compute Bézout's identity for the pairs $(30, 45)$, $(21, 321)$.
2. Programming part :
   - Implement the Sieve of Erathostene algorithm to find prime numbers up to a certain number n. Why don't we use it nowadays to find big prime numbers ?
   - Implement an algorithm bezout_coefficient(a,b) that takes two integers (a, b) as input and returns three integers (x, y, d) such that $a \cdot x + b \cdot y = d$ where d is the gcd of a and b.

Exercise 2 : Multiplicative groups revisited

1. By hand :
   - Compute $\mathbb{Z}_{10}^*$ and match each element with its inverse.
   - Do the same for $\mathbb{Z}_{11}^*$.
   - Show that $(n-1) \in \mathbb{Z}_n^*$ for any n and give its inverse.
   - Compute the multiplicative inverse of 23 modulo 64 using Bézout identity.

2. Programming part :

   - Implement a function multiplicative_inverse(x,m) that computes the inverse of x modulo m.