TP Python - Attaque d'Håstad

December 2, 2025

Le TP devra être rendu sous forme d'un notebook Python et sa qualité sera prise en compte pour la détermination d'un bonus

1 Mise en place

1. Implémenter (sans l'aide d'internet) l'algorithme d'euclide étendu.
2. *Vous avez intercepté trois messages chiffrés avec le cryptosystème RSA,* c_1, c_2, c_3*, dont on sait qu'ils chiffrent tous le même message* m*. Les messages ont respectivement été chiffrés avec les clés publiques suivantes :* $(3, N_1), (3, N_2), (3, N_3)$

   Reformuler l'énoncé si dessous comme un système de congruences.
3. Implémenter une fonction retournant u_i, l'inverse modulaire de $\hat{N}_i$ modulo N_i où $\hat{N}_i = \frac{N_1 \cdot N_2 \cdot N_3}{N_i}$, pour $i \in \{1, 2, 3\}$
4. Implémenter le théorème des restes chinois de sorte à calculer $m^3 \mod N_1 \cdot N_2 \cdot N_3$.
5. Justifier que l'on a $m^3 = (m^3 \mod N_1 \cdot N_2 \cdot N_3)$ et adaptez votre programme pour qu'il retourne m.

2 Mise en pratique

A l'aide de la documentation, de la mise en place et des fichiers dans le dossier Håstad, retrouver m.