

TD : RSA et algorithmes de factorisation

Romain Lebreton

09 novembre 2017

1. Génération de clé RSA

Une suggestion pour accélérer la génération de clé RSA et de prendre le produit de petits nombres premiers et de rajouter un (et bien sûr de vérifier que le résultat est premier). Que pensez-vous de cette méthode ?

2. Un exemple pour l'algorithme Pollard $p - 1$

Codez l'algorithme de Pollard $p - 1$ en Python et utilisez le pour factoriser complètement $N = 15770708441$.

3. Un exemple pour l'algorithme Pollard ρ

Soit $N = 7171$ et prenons la fonction pseudo-aléatoire $F(x) = x^2 + 1$. Calculez la suite des $x_i = F^{(i-1)}(x_1)$ pour $x_1 = 1$ et la suite des x'_i jusqu'à ce que $\text{pgcd}(x_i, x'_i) \notin \{1, N\}$. Déduisez-en un facteur p de N . Donnez la longueur s du cycle et celle r de la queue du ρ formé par les $(x_i \bmod p)$. Vérifiez les calculs du cours qui donnent l'indice de la première collision en fonction de r et de s .