Table des matières

1. Introduction

- 1.1 Formules mathématiques
- 1.2 Équations
- 1.3 Environnements
- 1.4 Faire référence

2. Divers

- 2.1 Enumérations
- 2.2 Tableaux
- 2.3 Polices

3. Système RSA

3.1 Fonctionnement

- 3.1.1 Comment ça marche
- 3.1.2 Démonstration
- 3.1.3 Application

3.2 Optimisation

- 3.2.1 La fonction indicatrice d'Euler φ et Indicatrice de Carmichael λ (évaluation de complexite avec des images de distribution)
- 3.2.2 Fast exponentiation, divide and conquer, version itérative et récursive (évaluation de complexité)
- 3.3.3 Algorithme d'Euclide étendu pour trouver l'inverse modulaire

4. Grands nombres premiers

4.1 Famille de nombres premiers et nombres pseudo-premiers

- 4.1.1 Nombres de Mersenne, de Fermat, ...
- 4.1.2 Sous-partie

4.2 Test de primalité (implémentation, analyse de complexité, application, etc.)

- 4.2.1 Tests déterministes
- 4.2.2 Tests probabilistes(Fermat, Miller-Rabin)

5. Extension et approfondissement

5.1 Hypothèse de Riemann généralisée

- 4.1.1 Miller-Rabin mais déterministe
- 4.1.2 Sous-partie

5.2 AKS algo(Prime is in P)

- 5.2.1 Premier test de primalité déterministe en temps polynomial sans se baser sur des conjectures mathématiques
- 5.2.2 Raisons pour lesquelles l'algorithme n'est pas largement adopté