université de BORDEAUX

PROJET TUTORÉ :

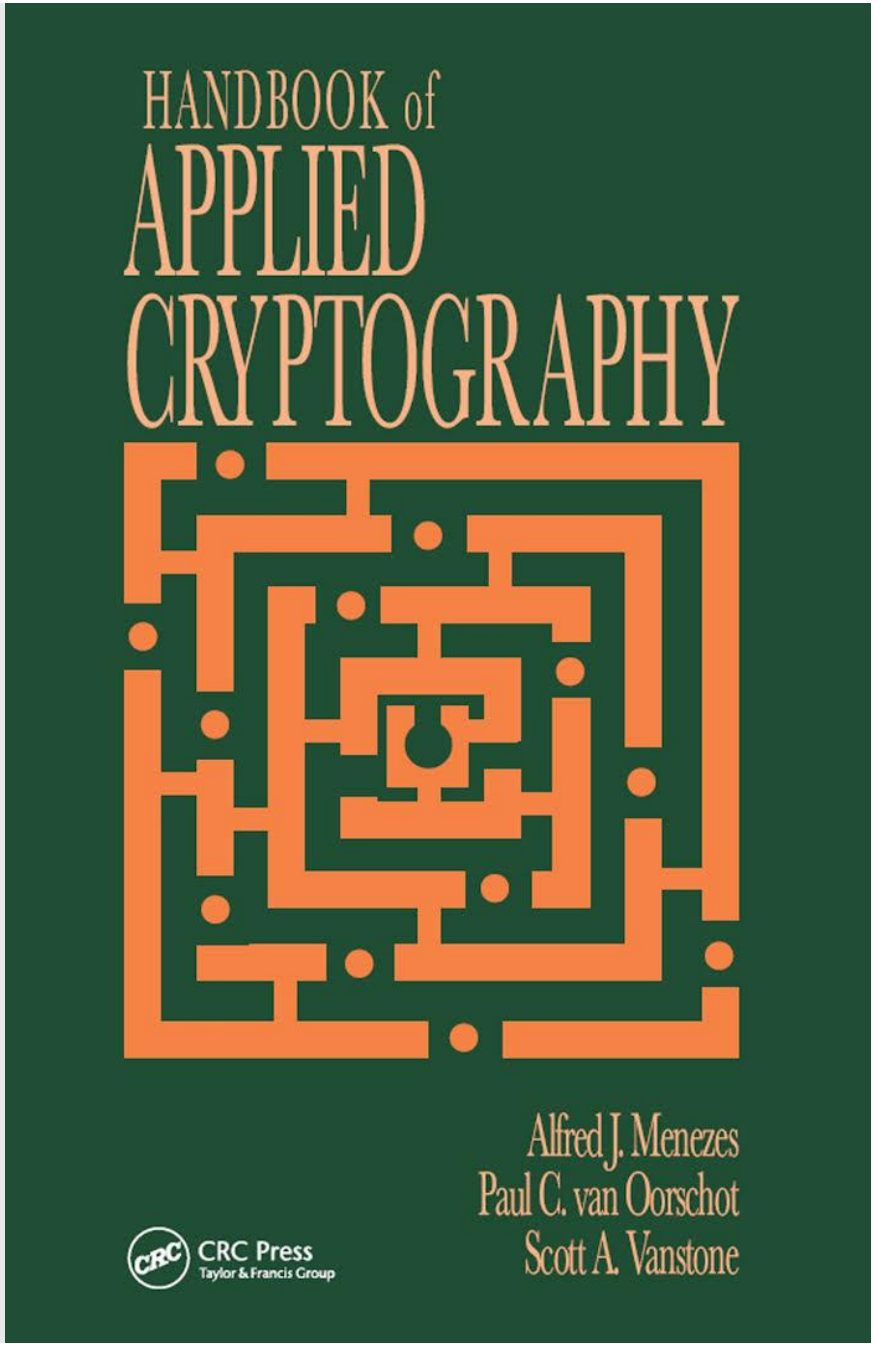
GÉNÉRATION ALÉATOIRE DE NOMBRE PREMIERS.

Toky RANDRIAMALALA
Elias DEBEYSSAC
Pierre GRABER

Année 2019-2020

Introduction

- Contexte
- Motivations du projet
- Liens direct avec le cours : Arithmétique et Cryptologie
  - Modules RSA, Signature Digitale



Sommaire

PREMIÈRE PARTIE

Pourquoi SageMath ?

- Langage Python :
  - Haut niveau
  - Déjà manipulé

- Logiciel Libre de calcul Mathématique
- Fonctions algebriques déjà implémentées
  - Exponentiation modulaire
  - Tests de primalité, Pseudo-Primalité

Les Tests de Primalité :

Divisions Successives

Miller-Rabin

Tests fournis par Sage :

- is_prime()
- is_pseudoprime()

SECONDE PARTIE

Premier Algorithme : Recherche Aléatoire

Algorithme simple

Boucle "Tant que" :

- Tirage aléatoire
- Test de Primalité

Génération de "Strong Prime"

Algorithme de Gordon

Premiers forts :

- (p-1) et (p+1) ont des "grands" facteurs premiers
- Te

Besoin de modules RSA surs

- Eviter la factorisation de (p-1) et (p+1)

Génération de "Strong Prime"

Algorithme de Gordon

Premiers forts :

- (p-1) et (p+1) ont des "grands" facteurs premiers
- Te

Besoin de modules RSA surs

- Eviter la factorisation de (p-1) et (p+1)