TP2

September 2022

1 Introduction

Objectif: mettre en pratique les connaissances théoriques vues en cours et en TD papier.
Prérequis:

- Savoir décrire le fonctionnement de RSA
- Être capable d'effectuer des opérations sur un ensemble Z/nZ

Connaissances à acquérir:

- Être capable d'implémenter une méthode de chiffrement asymétrique

Instructions: Réaliser ces exercices seul.

1.1 Chiffrement RSA - from scratch

Dans cet exercice, il est demandé de développer deux fonctions permettant de chiffrer et déchiffrer des messages avec RSA en utilisant le pseudo code déjà écrit lors de la s"ance de TD papier. Le paramétrage de RSA est laissé à la discrétion des développeurs.

1.2 Chiffrement RSA - package python

Maintenant que vous maîtrisez RSA, vous devez savoir utiliser les outils haut niveaux disponibles sur internet. Utilisez le package *rsa-python 0.1.1* disponible à l'adresse suivante: *https://pypi.org/project/rsa-python/* pour re-développer vos deux fonctions.

1.3 Pour aller plus loin

Réutilisez ces deux fonctions pour développer une application console implémentée en programmation orientée objet permettant de chiffrer et déchiffrer des messages. L'application console prendra en paramètre un message et un mode de fonctionnement (chiffrer ou déchiffrer) et retournera en sur la sortie standard le message chiffré ou déchiffré correspondant au message d'entrée.