SORBONNE UNIVERSITÉ

Cryptologie RSA

Version du 20 mars 2024

TME

Exercice 1 – Cryptographie RSA

Dans tout cet exercice on s'intéresse au cryptosystème RSA.

1. Implémenter le chiffrement et le déchiffrement RSA en utilisant une bibliothèque de grands entiers si nécessaire.
2. Implémenter le théorème des restes chinois (CRT) pour deux équations.
3. Implémenter une version CRT du cryptosystème RSA.
4. Faites un tableau de temps pour comparer vos deux implémentations de RSA en fonction de la taille du module utilisé (de 256 à 4096 bits).

Exercice 2 – Attaque RSA par Wiener

Dans tout cet exercice on s'intéresse à la cryptanalyse de RSA.

1. Soit a et b deux entiers premiers entre eux. Implémenter une fonction permettant de calculer la représentation en fraction continue de $\frac{a}{b}$.
2. Implémenter l'attaque de Wiener.
3. Utiliser votre implémentation de la question précédente pour tester des instances de RSA en fonction de la taille de l'exposant secret utilisé.

