Baptiste Cottier
baptiste.cottier@icloud.com
INSA - Hauts de France
2 décembre 2025

Chiffrement asymétrique

Exercice 1. Le cryptosystème RSA

A – Chiffrement du message m avec les paramètres suivants $p = 7$, $q = 13$, $e = 5$, $m = 9$.

- Quels critères doit-on vérifier sur p et q pour que le cryptosystème soit fonctionnel ?
- Déterminer N et $\varphi(N)$.
- Vérifier que e est premier avec $\varphi(N)$.
- Quelle est la clé publique ? la clé secrète ?
- Chiffrer m en calculant $m^e \mod N$.

B – Déchiffrement du message c avec les paramètres suivants $N = 77$, $e = 17$, $c = 57$.

- Déterminer p, q et $\varphi(N)$.
- Calculer d l'inverse de e modulo $\varphi(N)$ à l'aide de l'algorithme d'Euclide étendu et du théorème de Bezout.
- Déchiffrer c en calculant $c^d \mod N$.

C – Générer des paramètres valides pour réaliser une signature et une vérification de signature.

Exercice 2 – Optimisation : Théorème des Restes Chinois. On trouve le problème suivant de le *Sunzi suanjing*, un livre du 3e siècle écrit par le mathematicien Sun-Tzu:

> *Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?*

1 – Réécrire le problème comme un système de trois équations où chaque équation est de la forme : $x \equiv a_i \mod n_i$

2 – Calculer $\hat{n_i} = (n_1 \times n_2 \times n_3)/n_i$ for $i \in \{1, 2, 3\}$

3 – Pour $i \in \{1, 2, 3\}$, déterminer k_i tel que $k_i \times \hat{n_i} \equiv 1 \mod n_i$. On définit $e_i = k_i \times \hat{n_i}$

4 – Calculer $\sum_{i=1}^{3} a_i \times e_i$ et vérifier que la valeur obtenue est bien solution du système de la question 1.

5 – Est-ce la seule solution ?

Baptiste Cottier
baptiste.cottier@icloud.com
INSA - Hauts de France
2 décembre 2025

Application au déchiffrement de RSA. Le déchiffrement dans l'algorithme RSA consiste à calculer le chiffré à une grand puissance. Et plus l'exposant est grand, plus le déchiffrement prend du temps. Pour optimiser le temps de déchiffrement, on peut utiliser le *Théorème des Restes Chinois*.

On considère les paramètres suivants : $p = 7, q = 11$ et on veut déchiffer $c = 5$ avec la clé secrète $d = 53$. L'opération classique consiste à calculer $m = c^d \mod (p \times q)$. Le théorème des Restes Chinois nous permet de calculer m à partir de $m_p = m \mod p$ et $m_q = m \mod q$. On calcule m_p ainsi :

$$\begin{aligned} m_p &= m \mod p \\ &= (c^d \mod n) \mod p \\ &= c^d \mod p \\ &= c^{d \mod (p-1)} \mod p \end{aligned}$$

et analogiquement pour m_q.

6 – Calculer $d_p = d \mod (p-1)$ et $d_q = d \mod (q-1)$

7 – Calculer $m_p = c^{d_p} \mod p$ et $m_q = c^{d_q} \mod q$

8 – Appliquer le théorème des restes chinois pour retrouver m