Introduction à l'algorithme RSA

L'algorithme RSA (Rivest-Shamir-Adleman) est l'un des piliers de la cryptographie moderne et de la sécurité des communications sur Internet. C'est un algorithme de **cryptographie asymétrique**, ce qui signifie qu'il utilise deux clés distinctes : une clé publique pour chiffrer les données et une clé privée pour les déchiffrer.

La sécurité de RSA repose sur la **difficulté de factoriser de grands nombres premiers**. Dans des applications réelles, les nombres premiers p et q sont extrêmement grands (souvent de centaines de chiffres) pour garantir la robustesse du système de sécurité. Ces grands nombres rendent le processus de factorisation très difficile, ce qui rend RSA extrêmement sécurisé, à condition d'utiliser des clés suffisamment longues.

Cependant, pour des raisons pédagogiques, cet exercice utilise des valeurs simples de p et q afin de vous permettre de comprendre la logique sous-jacente de l'algorithme sans être submergé par des calculs complexes. Dans un contexte réel, les valeurs de p et q seraient beaucoup plus grandes pour assurer un niveau de sécurité élevé.

Objectif de l'exercice

Cet exercice vise à vous faire comprendre les étapes de base de l'algorithme RSA, en appliquant directement les calculs nécessaires pour :

1. **Générer une paire de clés RSA** en utilisant deux petits nombres premiers p et q.
2. **Chiffrer un message** à l'aide de la clé publique.
3. **Déchiffrer le message** à l'aide de la clé privée.

Exemple :

Dans cet exemple, je vais vous appliquer l'algorithme RSA pour chiffrer un message simple M , qui sera ici une petite valeur numérique pour simplifier l'exercice. En réalité, les messages que l'on chiffre sont bien plus complexes et peuvent contenir des données textuelles, des fichiers ou d'autres informations, souvent converties en une séquence de nombres avant d'être chiffrées. Ce cas pratique vous permettra de comprendre les étapes sous-jacentes du chiffrement et du déchiffrement dans RSA, tout en restant simple et pédagogique.

Objectif :

Le scénario de cet exemple consiste à chiffrer un message dans le cadre d'une communication sécurisée.

Soit :
M le message en clair à chiffrer et **C** le message chiffré du méssage M.
On ulilisera la Clef publique $\mathbf{K_1}$, et la Clef privée $\mathbf{K_2}$ et la Fonction de chiffrement:
$\mathbf{C_{K_1}(M)}$ et la Fonction de déchiffrement: $\mathbf{D_{K_2}(C)}$

Pour envoyer un message M on utilise la clef publique K_1 pour chiffrer M et on envoie le message C(Chiffré):

$$C = C_{K_1}(M)$$

A la réception du message chiffré C on utilise la clef privée K_2 pour déchiffrer le message C:

$$M = D_{K_2}(C)$$

Étape 1 :

Génération des clés

Pour cet exercice, nous allons utiliser les nombres premiers suivants :

- p=3
- q=7

Nous allons maintenant procéder aux calculs pour générer les clés RSA :

- Calculez $n=p\times q$ =21 **n=21**
- Calculez $\varphi(n)=(p-1)\times(q-1)$= 12 **φ(n)=12**
- Choisissez un entier **e** tel que $1<e<\varphi(n)$ et que e soit premier avec φ(n). Nous choisirons pour 1<e< 12 **e=5.**
- Calculez d, l'inverse multiplicatif de e modulo φ(n), c'est-à-dire $e\times d\equiv 1 (\mathrm{mod}\varphi(n))$. Nous choisirons **d=5.**

Ainsi, vous obtiendrez :

- **Clé publique** : (n,e)=(21,5)
- **Clé privée** : (n,d)=(21,5)
-

Une fois les clés générées, vous allez chiffrer le message M. , nous allons associer une lettre de l'alphabet à un nombre entre 1 et 26 (A = 1, B = 2, ..., Z = 26).

Le message à chiffrer est la lettre **B,** ce qui correspond à Méssage**=M=2**. en utilisant la Clé publique :**(21,5) et**

Clé privée **:(21,5)** générées précedement.

Étape 2 : Chiffrement du message

Nous voulons chiffrer le message **B**, qui correspond à m=2.

Le chiffrement se fait selon la formule suivante :

$F_{K1}(M) = C = M^e \bmod n = 2^5 \bmod 21 = 32 \bmod 21 = 11$, Donc le message chiffré est **C=11**

Le message chiffré C est donc 11 : **C=11**

Étape 3 : Déchiffrement du message

Maintenant, pour déchiffrer le message, on utilise la clé privée et la formule suivante :

$D_{K1}(C) = C^d \bmod n = 11^5 \bmod 21 = 161051 \bmod 21 = 2$ D=2=M
Le message déchiffré M est donc 2, ce qui correspond à la lettre **B**.

Vous pouvez voir qu'en utilisant la clé publique pour chiffrer et la clé privée pour déchiffrer, vous récupérez le message original.