Solution pour trouver la clé privée dans l'exercice RSA

Nous cherchons à trouver un entier d tel que $7d \equiv 1 \pmod{160}$.

Cela signifie que $7d-1$ est un multiple de 160, ou en d'autres termes, il existe un entier k tel que $7d-1=160k$.

Notre objectif est de trouver la valeur de d.

Pour résoudre cette congruence linéaire, nous pouvons utiliser l'algorithme d'Euclide étendu.

Cet algorithme nous permet de trouver des entiers x et y tels que $\text{pgcd}(a,b)=ax+by$.

Dans notre cas, a=7 et b=160.

Si le pgcd (7,160)=1, alors une solution d existe.

Étape 1 : Appliquer l'algorithme d'Euclide pour trouver le pgcd (7, 160)

1. $160=22\times7+6$
2. $7=1\times6+1$
3. $6=6\times1+0$

Le dernier reste non nul est 1, donc pgcd (7, 160) =1. Cela confirme qu'une solution existe.

Étape 2 : Remonter l'algorithme d'Euclide pour exprimer le pgcd comme une combinaison linéaire de 7 et 160

À partir de la deuxième équation :

$1=7-1\times6$

Substituons l'expression de 6 à partir de la première équation ($6=160-22\times7$) dans l'équation ci-dessus :

$1=7-1\times (160-22\times7)$

$1=7-160+22\times7$

$1=23\times7-1\times160$

Nous avons donc trouvé que $23\times7-1\times160=1$.

Étape 3 : Interpréter la combinaison linéaire en termes de congruence

L'équation $23\times7-1\times160=1$ peut être réécrite sous la forme :

$23\times7=1+1\times160$

$23 \times 7 \equiv 1 \pmod{160}$

En comparant avec notre congruence de départ $7d \equiv 1 \pmod{160}$, nous voyons que $d=23$ est une solution.

Vérification :

$7 \times 23 = 161$

$161 \pmod{160} = 1$

Donc, $7 \times 23 \equiv 1 \pmod{160}$ est bien vérifié.

Conclusion :

La valeur de d qui satisfait la congruence $7d \equiv 1 \pmod{160}$ est $d = 23$.

Comment trouver le 23 :

Le "23" est apparu en remontant les étapes de l'algorithme d'Euclide étendu.

Nous avions les équations de l'algorithme d'Euclide :

1. $160 = 22 \times 7 + 6$
2. $7 = 1 \times 6 + 1$
3. $6 = 6 \times 1 + 0$

Notre objectif était d'exprimer le dernier reste non nul (qui est le pgcd, et ici il vaut 1) comme une combinaison linéaire de 7 et 160,

c'est-à-dire sous la forme $1 = 7x + 160y$ pour trouver les entiers x et y. La valeur de x sera notre d.

Voici comment nous avons "remonté" :

- À partir de la deuxième équation :

  Nous avons isolé le reste 1 :

  $1 = 7 - 1 \times 6$

- Substitution de la première équation dans l'expression de 1 :

  La première équation nous donne une expression pour le reste précédent, 6 :

  $6 = 160 - 22 \times 7$

Maintenant, nous substituons cette expression de 6 dans l'équation pour 1 :

$1=7-1\times(160-22\times7)$

- Simplification de l'expression :

  $1=7-1\times160-1\times(-22\times7)$

  $1=7-160+22\times7$

- Regroupement des termes contenant 7 :

  $1=(1\times7)+(22\times7)-1\times160$

  $1=(1+22)\times7-1\times160$

  $1=23\times7-1\times160$

  Ainsi, nous avons exprimé le pgcd (1) sous la forme $23\times7+(-1)\times160$.

  En comparant cela à la forme $7d\equiv1(\mathrm{mod}160)$, qui est équivalente à $7d-1=160k$ (ou $7d=1+160k$), nous voyons que si nous prenons $d=23$ et $k=1$, l'équation est satisfaite :

  $7\times23=1+160\times1$

  $161=1+160$

  $161=161$

  Donc, le coefficient de 7 dans notre combinaison linéaire (qui est 23) est la solution d que nous recherchions.