Utilisation du théorème du reste chinois dans RSA

Mauvaise exponentiation modulaire de RSA

Lorsque nous déroulons l'algorithme de l'exponentiation modulaire donné en cours nous constatons que le temps de calcul dépend de la taille de la clé mais surtout du nombre des bits 1 dans la clé privée. En effet à chaque fois où un bit=1, il y a une opération supplémentaire réalisée. L'attaquant peut ainsi connaître la clé privée à partir de l'activité du calculateur (attaque par canal auxiliaire) : Temps de calcul, consommation énergétique, analyse d'émanation électromagnétique… Simplement en mesurant les opérations réalisées, il peut savoir au moins le nombre de bit=1. En étant à proximité de l'unité de calcul, il peut même détecter les 1 et les zéros.

CRT : Chinese remainder theorem

Deux problèmes se posent lorsque l'on calcule directement $m = c^d \% n$ avec d étant la clé privée. Le premier est le temps de calculs qui est très long, le deuxième est dû à la possibilité d'écoute permettant de déduire la taille de la clé et le nombre de 1.
Le théorème du reste chinois (CTR) peut se formuler comme suit :

Soient

- $N=n_1 \times n_2 \ldots \times n_k$, *avec* n_i *et* n_j *sont deux à deux premiers entre eux pour tout* $i \neq j$ *avec* $i,j \in [1,k]$,
- $x_1, x_2 \ldots, x_k$ *tel que* $0 \leq x_i < n_i$ *avec* $i \in [1,k]$

Alors,

- *Il existe une solution unique* $0 \leq x < N$ *telle que* $x \equiv x_i mod(n_i)$ *ou autrement écrit* $x_i = x \% n_i$ *pour tout* $i \in [1,k]$

Ainsi, à partir du CRT, puisque $n=p \times q$ nous considérons les deux résultats suivants :

- $m_p = c^d \% p$
- $m_q = c^d \% q$

Et nous cherchons la solution unique m à partir de m_p et m_q

Autrement dit, soit $C = c^d$, nous cherchons $m = C \% \left(\underbrace{\times}_{n} \right)$ avec selon CTR :

- $m_q = m \% q$, ce qui fait $m = m_q + h \times q$ ……(1)
- $m_p = m \% p$, ce qui fait $m = m_p + l \times p$ ……(2)

En remplaçant (1) dans (2), nous avons $h \times q = m_p - m_q + l \times p$. Autrement dit :

- $(h \times q) \% p = mp - mq$……(3)

Pour obtenir h, il suffit de multiplier (3) par l'inverse de q dans $\mathbb{Z}_p$ que nous notons q^{-1}. On calcule l'inverse de q grâce à l'algorithme d'Euclide généralisé. Ainsi nous avons :

- $h = ((m_p - m_q) q^{-1}) \% p$……(4)

Pour obtenir m il suffit de calculer d'après (1) et (4) :

$$m = (m_q + h \times q) \% n \ldots\ldots (5)$$

Pour la simplification du calcul de $m_q = c^d \% q$ et de $m_p = c^d \% p$, il suffit de calculer $m_q = c^{d_q} \% q$ et $m_p = c^{d_p} \% p$ avec :

- $d_q = d \% \varphi(q)$ et $d_p = d \% \varphi(p)$,

- $\varphi(*)$ désignant l'indicatrice d'Euler. Puisque q et p sont premiers nous avons $\varphi(q)=q-1$ et $\varphi(p)=p-1$.

En effet, nous savons d'après le théorème d'Euler, $c\varphi(k)\%k=1$

Algorithme de calcul $m = c^d\%n$ en utilisant CRT

Calcul préalable :

1- Avec $n = x_i x_j$ prendre $q = x_i$ et $p = x_j$ tel que $x_i < x_j$
2- Calculer q^{-1} dans $\mathbb{Z}_p$
3- Calculer d_q=$d\%(q\text{-}1)$ et d_p=$d\%(p\text{-}1)$

Ces calculs sont réalisés **qu'une seule fois** et les valeurs de q^{-1}, d_q et d_p sont gardées secrètement.

A la réception d'un message c, effectuer les opérations suivantes :

1- Calculer $m_q = c^{d_q}\%q$ et $m_p = c^{d_p}\%p$
2- Calculer $h = \left((m_p - m_q)q^{-1}\right)\%p$
3- Calculer $m = \left(m_q + h \times q\right)\%n$

Exemple

On déroule ici l'algorithme sur l'exemple de déchiffrement suivant : m= $8363^{11787}\%17947$ avec 17947=137x131

On choisit q comme étant la plus petite valeur des facteurs de n, à savoir entre 137 et 131

On commence par le calcul de $d_p=d\%\varphi(p)$ et de $d_q=d\%\varphi(q)$ que l'on garde pour la suite

$\boldsymbol{d_p}=d\%\varphi(p)=11787\%136=\mathbf{91}$, $\boldsymbol{d_q}=d\%\varphi(q)=11787\%130=\mathbf{87}$

On calcul q^{-1} avec l'algorithme d'Euclide étendu :

Etapes	r	nouvr	quotient	t	nouvt
0	**137**	**131**	137//131=1	**0**	**1**
1	**131**	137%131=**6**	131//6=21	**1**	0-(1*1)=**-1**
2	**6**	131%6=**5**	6//5=1	**-1**	1-(-1*21)=**22**
3	**5**	**1**		**22**	-1-(1*22)=**-23**

q^{-1}=−23%137=**114**

Nous avons ainsi $\boldsymbol{d_p}$= **91**, $\boldsymbol{d_q}$=**87** et $\boldsymbol{q^{-1}}$=**114**

On calcule en premier m_p et m_q :

$m_p=c_{d_p}\%p=(8363^{91})\%137=102$

$m_q=c_{d_q}\%q=(8363^{87})\%131=120$

Pour obtenir le message m on doit calculer : $h=((m_p-m_q)q^{1})\%p=((102-120)\ 114)\%137=3$

Nous obtenons ainsi $m=(m_q+h\times q)\%n=(120+3*131)\%17947=513$

Question : s'agit-il du message original ?

Avec $d = 11787$ on a $e = 3$. En effet, nous avons :

- $e \times d = 11787 \times 3 = 35361$
- et $35361\%(17680) = 1$.

$513^3\%17947$=8363 et c'est bien le message chiffré reçu initialement.