Rappel sur RSA

p, q sont deux grands nombres premiers distincts.

$$N = p * q$$

$$\Phi(n) = (p-1)(q-1)$$

$$E : \text{PGCD}(e, \Phi(n)) = 1$$

$$D : e * d \text{ modulo } \Phi(n) = 1 \text{ (ou de manière équivalente, } e * d \equiv 1 [\Phi(n)])$$

Clé publique : (n, e) Formule de chiffrement : $C = M^e \text{ mod } n$

Clé privée : (n, d) Formule de déchiffrement : $M = C^d \text{ mod } n$

C : texte chiffré

M : texte clair

Exercice 2 serie 3.2 : RSA

1) Déchiffrement du message $m = 18$ chiffré avec la clé publique $(35, 11)$.

Il faut trouver la clé privée pour le déchiffrement.

Nous avons:

$$e = 11 \text{ et } n = 35.$$

$$n = 7 * 5 = p * q.$$

Pour trouver d , nous appliquons l'algorithme d'Euclide étendu :

$$E * d \equiv 1 [\Phi(n)] \text{ alors } 11 * d \equiv 1 [24].$$

Nous exprimons 24 en utilisant la valeur de e .

Alors,

$$24 = 11 * 2 + 2$$

$$\Rightarrow 2 = 24 - 11 * 2$$

$$11 = 2 * 5 + 1$$

$$\Rightarrow 1 = 11 - 2 * 5$$

$$2 = 1 * 2 + 0$$

le reste = 0, on arrête.

Dernière équation avec un reste non nul: $1 = 11 - 2 * 5$

et on remplace 2 à partir de l'équation précédente

$$1 = 11 - (24 - 11 * 2) * 5$$

$$1 = 11 - 5 * 24 + 11 * 10$$

$$1 = 11 * 11 - 5 * 24 \quad \Rightarrow \quad 1 = e * 11 - 5 * 24 \text{ alors } d = 11$$

Si le résultat de $d < 0$, on ajoute $\Phi(n)$ à d . Dans ce résultat, nous n'avons pas besoin d'ajouter $\Phi(n)$.

$$D = 11$$

$$C = 18$$

$$M = 18^{11} \text{ modulo } 35$$

Si le résultat ne peut pas être calculé avec une calculatrice, suivez la méthode suivante:

$$M = 18^{11} \text{ modulo } 35$$

Nous écrivons 11 sous forme d'addition de nombres qui peuvent être exprimés en tant que 2^k : $11=8+2+1$
 $M = 18^{11} \text{ modulo } 35 = 18^{8+2+1} \text{ modulo } 35$

$$\begin{aligned} 18^1 \text{ modulo } 35 &= 18 \\ 18^2 \text{ modulo } 35 &= 9 \\ 18^8 \text{ modulo } 35 &= 18^2 * 4 \text{ modulo } 35 \\ &= (18^2)^4 \text{ modulo } 35 \\ &= (18^2 \text{ modulo } 35)^4 \text{ modulo } 35 \\ &= (9)^4 \text{ modulo } 35 \\ &= 16 \end{aligned}$$

$$\begin{aligned} M &= 18^{11} \text{ modulo } 35 = (18 * 9 * 16) \text{ modulo } 35 \\ &= 2 \text{ modulo } 35 \\ &= 2 \end{aligned}$$

Pour vérifier ce résultat (la valeur de **d**), nous pouvons confirmer en testant différentes valeurs de d dans l'équation:

$$11d \text{ mod } 24=1$$

Pour cela, nous allons simplement tester les différentes valeurs de d:

$$\begin{aligned} d=1 &\Rightarrow 11 \times 1 \text{ mod } 24=11 \\ d=2 &\Rightarrow 11 \times 2 \text{ mod } 24=22 \\ d=3 &\Rightarrow 11 \times 3 \text{ mod } 24=9 \\ d=4 &\Rightarrow 11 \times 4 \text{ mod } 24=20 \\ d=5 &\Rightarrow 11 \times 5 \text{ mod } 24=3 \\ d=6 &\Rightarrow 11 \times 6 \text{ mod } 24=14 \\ d=7 &\Rightarrow 11 \times 7 \text{ mod } 24=5 \\ d=8 &\Rightarrow 11 \times 8 \text{ mod } 24=16 \\ d=9 &\Rightarrow 11 \times 9 \text{ mod } 24=7 \\ d=10 &\Rightarrow 11 \times 10 \text{ mod } 24=18 \\ d=11 &\Rightarrow 11 \times 11 \text{ mod } 24=1 \end{aligned}$$

(Voilà, nous avons trouvé $d=11 \text{ mod } 24$)

Donc, la valeur de d qui satisfait l'équation est 11.

2) Chiffrement du message $m = 10$ avec la clé publique (55, 7).

Nous avons:

$$E= 7 \text{ et } n=55 \text{ et } m=10.$$

$$C = M^e \text{ modulo } 55$$

$$C = 10^7 \text{ modulo } 55$$

Si le résultat ne peut pas être calculé avec une calculatrice, suivez la méthode suivante:

$$C = 10^7 \text{ modulo } 55$$

Nous écrivons 7 sous forme d'addition de nombres qui peuvent être exprimés en tant que 2^k : $7=4+2+1$

$$\begin{aligned}M &= 10^7 \text{ modulo } 55 = 10^{4+2+1} \text{ modulo } 55 \\10^1 \text{ Modulo } 55 &= 10 \\10^2 \text{ Modulo } 55 &= 45 \\10^4 \text{ modulo } 55 &= 10^2 * 2 \text{ modulo } 55 \\&= (10^2)^2 \text{ modulo } 55 \\&= (10^2 \text{ modulo } 55)^2 \text{ modulo } 55 \\&= (45)^2 \text{ modulo } 55 \\&= 45\end{aligned}$$

$$\begin{aligned}C &= 10^7 \text{ modulo } 55 = (10 * 45 * 45) \text{ modulo } 55 \\&= 10 \text{ modulo } 55 \\&= 10\end{aligned}$$

Donc le message chiffré est $C = 10$

2) Calculer p ; q et d .

$$\begin{aligned}n &= 55 = 5 * 11 \Rightarrow p = 5 \text{ et } q = 11 \\ \Phi(n) &= (p - 1) (q - 1) = 4 * 10 = 40\end{aligned}$$

$$e = 7$$

pour trouver d on a :

$$e * d \equiv 1 \text{ } [\Phi(n)] \text{ alors } 7 * d \equiv 1 \text{ } [40].$$

Nous exprimons $\Phi(n)$ en utilisant la valeur de 'e'.

$$\text{Alors, } 40 = 7 * 5 + 5 \quad \Rightarrow \quad 5 = 40 - 7 * 5$$

$$7 = 5 * 1 + 2 \quad \Rightarrow \quad 2 = 7 - 5 * 1$$

$$5 = 2 * 2 + 1 \quad \Rightarrow \quad 1 = 5 - 2 * 2$$

$$2 = 1 * 2 + 0 \quad \text{le reste} = 0, \text{ on arrête.}$$

Dernière équation avec un reste non nul: $1 = 5 - 2 * 2$

et on remplace 2 à partir de l'équation précédente.

$$\begin{aligned}1 &= 5 - 2 * (7 - 5 * 1) \\1 &= 5 - 2*7 + 2*5 \\&= 5*3 - 2*7 \text{ on remplace } 5 \text{ à partir de l'équation } 5 = 40 - 7 * 5. \\1 &= (40 - 7*5)*3 - 2*7 \\&= 40*3 - 7*15 - 2*7 \\&= 40*3 + 7* (-17) \quad \Rightarrow \quad 1 = e * (-17) + 40 * 3\end{aligned}$$

$-17 < 0$, on ajoute $\Phi(n)$ à -17 . $40 - 17 = 23$ alors $d = 23$

Pour vérifier ce résultat (la valeur de d), nous pouvons le vérifier en suivant la démarche suivante :

$$11d \bmod 24 = 1$$

L'équation $(11 \times d) \bmod 24 = 1$ indique que lorsque vous multipliez 11 par d et prenez le reste de cette multiplication après la division par 24, le résultat est égal à 1.

Cela peut être exprimé comme $11 \times d = 24 \times k + 1$, où k représente le quotient de la division entière de $11 \times d$ par 24

$$11 \times d = 24 \times k + 1$$

$$\text{Alors } d = (24 \times k + 1) / 11 \quad \text{''Sachant que d et k sont des entiers''}$$

Pour cela, nous allons simplement tester différentes valeurs de k jusqu'à ce que nous trouvions une valeur entière de d.

$$d = (24 \times k + 1) / 11$$

k=1	⇒	d=5.85	(refuse´)
k=2	⇒	d=11.57	(refuse´)
k=3	⇒	d=17.28	(refuse´)
k=4	⇒	d=23	(accepte´)

(Ainsi, nous avons trouvé **d= 23 mod 40**)

Donc, la valeur de d qui satisfait l'équation est 23.

2) Déchiffrer C = 35

Clé privée (55, 23)

C=35

$M = C^d \bmod n$

$$M = 35^{23} \bmod 55$$

Nous écrivons 23 sous forme d'addition de nombres qui peuvent être exprimés en tant que 2^k : $23 = 16 + 4 + 2 + 1$

$$M = 35^{23} \bmod 55 = 35^{16 + 4 + 2 + 1} \bmod 55$$

$$35^1 \bmod 55 = 35$$

$$35^2 \bmod 55 = 15$$

$$\begin{aligned} 35^4 \bmod 55 &= 35^2 * 2 \bmod 55 \\ &= (35^2)^2 \bmod 55 \\ &= (35^2 \bmod 55)^2 \bmod 55 \\ &= (15)^2 \bmod 55 \\ &= 5 \end{aligned}$$

$$\begin{aligned} 35^{16} \bmod 55 &= 35^4 * 4 \bmod 55 \\ &= (35^4)^4 \bmod 55 \\ &= (35^4 \bmod 55)^4 \bmod 55 \\ &= (5)^4 \bmod 55 \\ &= 20 \end{aligned}$$

$$\begin{aligned} M &= 35^{23} \text{ modulo } 55 = (35 * 15 * 5 * 20) \text{ modulo } 55 \\ &= 30 \text{ modulo } 55 \\ &= \mathbf{30} \end{aligned}$$

Le message clair est donc: **M= 30**