

1. Rappeler que $\pi : \mathbb{Z}/pq\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, où $\pi(x) = (x \bmod p, x \bmod q)$ est un bijection pour p et q premiers entre eux, et supposer que $up + vq = 1$.

- a. Vérifier que $\pi(x + y) = \pi(x) + \pi(y)$ et $\pi(xy) = \pi(x)\pi(y)$, où

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2),$$

et conclure que $\pi(x^k) = \pi(x)^k$.

- b. Montrer que $x_1 + (x_2 - x_1)up = x_2 + (x_1 - x_2)vq$ et que l'application

$$\iota(x_1, x_2) = x_1 + (x_2 - x_1)up$$

est l'inverse de π .

- c. Si $k = r(p - 1)$ pour un entier r , montrer que $\text{pgcd}(x^k - 1, pq)$ est divisible par p pour tout x tel que $x \bmod p \neq 0$. Est-ce que ça pose un problème pour RSA ? Pourquoi ou pourquoi pas ?

Solution.

- a. Les identités $\pi(x+y) = \pi(x) + \pi(y)$ et $\pi(xy) = \pi(x)\pi(y)$, sont des conséquences du fait que l'addition et la multiplication sont bien définies modulo p et q (et que la fonction π est bien définie). Par conséquence, $\pi(x^k) = \pi(x) \cdots \pi(x) = \pi(x)^k$.
- b. L'égalité $x_1 + (x_2 - x_1)up = x_2 + (x_1 - x_2)vq$ devient

$$(x_2 - x_1)(up + vq - 1) = 0,$$

qui est vérifiée pour tout x_1 et x_2 . On vérifie alors que $\iota(x_1, x_2)$ est aussi égale à $x_2 + (x_1 - x_2)vq$, et donc

$$(\iota(x_1, x_2) \bmod p, \iota(x_1, x_2) \bmod q) = (x_1, x_2).$$

- c. Même si un tel pgcd détermine une factorisation de pq , il ne pose pas de problème car la probabilité de tomber sur un tel entier k est trop faible $1/(p-1)$. C'est presque la même probabilité de trouver une factorisation avec $\text{pgcd}(a, pq)$, en choisissant un entier a au hasard.

2. Supposer que $p = 7$ et $q = 11$, avec π comme au-dessus, et que $e = 17$.

- a. Trouver d tel que $ed \bmod \text{ppcm}(p - 1, q - 1) = 1$.
- b. Trouver c tel que $\pi(c) = (3, 1)$.
- c. Calculer $(3, 1)^d$ dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ et trouver m tel que $\pi(m) = (3, 1)^d$.
- d. Vérifier que $m^e = c$ dans $\mathbb{Z}/pq\mathbb{Z}$.

Solution.

- a. Nous trouvons $1 = -7 \cdot 17 + 2 \cdot 60$, donc $d = -7 \bmod 60 = 53$ est l'inverse de e modulo $\text{ppcm}(p-1, q-1) = 60$.
- b. Le pgcd étendu de 7 et 11 est $1 = -3 \cdot 7 + 2 \cdot 11$, donc

$$\iota(x_1, x_2) = x_1 - 21(x_2 - x_1) \bmod 77.$$

En particulier $\pi(3, 1) = 45$.

- c. Par définition, $(x_1, x_2)^d = (x_1^d, x_2^d)$, et on note que

$$(x_1^d, x_2^d) = (x_1^{d_1}, x_2^{d_2}),$$

où $d_1 = d \bmod p-1$ et $d_2 = d \bmod q-1$. Alors la puissance $(3, 1)^d$ est égale à $(3^{53}, 1) = (3^5, 1) = (5, 1)$, et donc

$$m = \pi(5, 1) = 5 - 21(1 - 5) \bmod 77 = (5 + 84) \bmod 77 = 12.$$

- d. Par les suites de carrés $(m, m^2, m^4, m^8, m^{16}) = (12, 67, 23, 67, 23)$, l'expression $12^{17} \bmod 77 = 45$ est vérifiée :

$$12^{17} \bmod 77 = (12 \cdot 12^{16}) \bmod 77 = (12 \cdot 23) \bmod 77 = 45.$$

3. Soit $p = 37$, $q = 43$ et $e = 65$, et alors $\text{ppcm}(p-1, q-1) = 36 \cdot 7 = 252$.
- a. En donnant $1 = -31e + 8 \cdot 252$, trouver $d > 0$ tel que $ed \bmod 252 = 1$.
- b. Trouver (u_1, v_1) tel que $1 = u_1e + v_1(p-1)$ et (u_2, v_2) tel que $1 = u_2e + v_2(q-1)$, et alors trouver $d_1 = e^{-1} \bmod (p-1)$ et $d_2 = e^{-1} \bmod (q-1)$.
- c. Vérifier que $d_1 = d \bmod (p-1)$ et $d_2 = d \bmod (q-1)$.

Solution.

- a. On a $d = 221 \bmod 252$.
- b. On trouve $1 = 5e - 9(p-1)$ et $1 = 11e - 17(q-1)$, alors $d_1 = 5$ et $d_2 = 11$.
- c. On a bien $5 = 221 \bmod (p-1)$ et $11 = 221 \bmod (q-1)$.
4. Pour les mêmes valeurs de p , q et e dans l'exercice précédent, soit $n = pq$ et prendre le message $m = 100$.
- a. Trouver $c = m^e \bmod n$, $c_1 = m^e \bmod p$ et $c_2 = m^e \bmod q$ et vérifier que $c = \iota(c_1, c_2)$.
- b. Trouver $s = m^d \bmod n$, $s_1 = m^{d_1} \bmod p$ et $s_2 = m^{d_2} \bmod q$ et vérifier que $s = \iota(s_1, s_2)$.
- c. Vérifier que s est la signature de m .
- d. Quels sont les étapes ci-dessus qui peuvent être fait avec la clé RSA publique et quels ont besoin de la clé privée ?

Solution. On a les valeurs $p = 37$, $q = 43$, $e = 65$ et $n = pq = 1591$.

- a. On trouve $c = 100^{65} \bmod 1591 = 454$, $c_1 = 100^{65} \bmod 37 = 10$, et $c_2 = 100^{65} \bmod 43 = 24$. En utilisant le resultat du pgcde, $7 \cdot 37 - 6 \cdot 43 = 1$, on vérifie l'égalité

$$c = 454 = c_1 + 7 \cdot 37(c_2 - c_1) \bmod 1591 = c_2 - 6 \cdot 43(c_1 - c_2) \bmod 1591.$$

Remarque : Ce calcul utilise la connaissance de la factorisation de n , qui n'est pas disponible à une personne qui fait un chiffrement.

- b. On sait que $d = 221$ et $(d_1, d_2) = (5, 11)$. On trouve $s = 100^{221} \bmod 1591 = 10$ compatible avec $(c_1, c_2) = (10, 10)$.

Remarque : La personne que fait la signature connaît la clé privée, ainsi que la factorisation de n .

- c. On vérifie que $s^e \bmod n = 10 \cdot 10^{64} \bmod 1591 = 100 = m$.

Remarque : Ce calcul sera plus facile modulo p et modulo q , mais ces entiers ne sont pas disponibles pour la personne que fait la vérification.

- d. Voir les remarques précédentes.

5. Soit $p = 59$, $a = 2$, et $b = 56$.

- a. Vérifier que $k = 21$ est la clé privée pour la clé publique ElGamal (p, a, b) .
 b. Calculer un chiffrement de $m = 7$ avec (p, a, b) . Pourquoi n'est-t-il pas unique ?
 c. Montrer les étapes pour déchiffrement de votre texte chiffré.

Solution.

- a. Il faut vérifier que $a^{21} \bmod 59 = 56$. Pour cela, on calcule les carrés successifs de a modulo 59 :

$$\begin{aligned} a &= 2 \\ a^2 &= 4 \\ a^4 &= 16 \\ a^8 &= 20 = 256 \bmod 59 \\ a^{16} &= 46 = 400 \bmod 59 \end{aligned}$$

et on exprime $a^{21} \bmod 59 = (a \cdot a^4 \cdot a^{16}) \bmod 59$:

$$\begin{aligned} (2 \cdot 16 \cdot 46) \bmod 59 &= (16 \cdot 96) \bmod 59 = (16 \cdot 33) \bmod 59 \\ &= (8 \cdot 66) \bmod 59 = (8 \cdot 7) \bmod 59 = 56. \end{aligned}$$

- b. Pour le chiffrement, il faut choisir un exposant ℓ , pour lequel on prend $\ell = 13$. Le texte chiffré est $(r, s) = (a^\ell \bmod p, mb^\ell \bmod p)$. En utilisant la méthode 'carré-et-multiplication', on trouve

$$(2^\ell \bmod 59, 56^\ell \bmod 59) = (50, 34),$$

et $2 = 7 \cdot 34 \bmod 59$. Donc le chiffrement est $(r, s) = (50, 2)$.

- c. Le déchiffrement est $m = r^{-k}s \bmod p$. L'inverse de 50 modulo 59 est 13, et $33 = 13^{21} \bmod 59$. Donc $33 = r^{-k} \bmod 59$, et $m = (33 \cdot 2) \bmod 59 = 7$.