

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 ?
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 $\mathbb{Z}/pq\mathbb{Z}$.
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 $d_2 = d \bmod (q - 1)$.
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 ?
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.