

Exercice 1. Soit $p = 59$, $q = 61$, et $e = 17$. Alors avec le pgcd étendu on trouve :

$$1 = -17e + 5(p - 1) \text{ et } 1 = -7e + 2(q - 1)$$

- a. Trouvez $d_1 = e^{-1} \bmod (p - 1)$ et $d_2 = e^{-1} \bmod (q - 1)$.

Solution. Les reductions $\bmod(p - 1)$ et $\bmod(q - 1)$ des equations sont :

$$1 = -17e + 5(p - 1) \bmod (p - 1) = -17e \bmod (p - 1) = 41e \bmod (p - 1),$$

et

$$1 = -7e + 2(q - 1) \bmod (q - 1) = -7e \bmod (q - 1) = 53e \bmod (q - 1),$$

alors $d_1 = 41$ et $d_2 = 53$.

- b. En donnant $2 = (-1) \cdot (p - 1) + 1 \cdot (q - 1)$, calculez un entier d tel que

$$ed \bmod \frac{(p - 1)}{2} = 1 \text{ et } ed \bmod \frac{(q - 1)}{2} = 1$$

Solution. Il suffit de trouver d tel que

$$d \bmod \frac{(p - 1)}{2} = 41 \bmod \frac{(p - 1)}{2} \text{ et } d \bmod \frac{(q - 1)}{2} = 53 \bmod \frac{(q - 1)}{2}.$$

L'équation donnée est équivalent au pgcd de $(p - 1)/2$ et $(q - 1)/2$:

$$1 = (-1) \cdot \frac{(p - 1)}{2} + 1 \cdot \frac{(q - 1)}{2},$$

Il faut résoudre les equations :

$$(i) d = d_1 + k_1 \frac{(p - 1)}{2} \text{ et } (ii) d \bmod \frac{(q - 1)}{2} = d_2 \bmod \frac{(q - 1)}{2}$$

qui a comme solution

$$k_1 = (-1)(d_2 - d_1) \bmod \frac{(q - 1)}{2} = -12 \frac{(q - 1)}{2} = 18.$$

Alors $d = 41 + 18(p - 1)/2 = 41 + 18 \cdot 29 = 563$.

c. Trouvez d tel que $ed = 1 \pmod{p-1}$ et $ed = 1 \pmod{q-1}$

Solution. Comme $d = 41 + 18 \cdot 29 = 41 + 9 \cdot 58$, la valeur de d est bonne mod $(p-1) = 58$ (et non seulement mod 29). Mais nous trouvons

$$41 + 9 \cdot 58 = 41 + 9 \cdot (-2 + 60) = 41 - 18 + 9 \cdot 60 = 23 + 9 \cdot 60,$$

alors $d \pmod{q-1} = 23$ n'est pas la bonne valeur 53.

Nous pouvons faire le calcul de d avec $\text{pgcd}(e, \phi(pq)) = \text{pgcd}(e, (p-1)(q-1))$:

$$1 = -2047e + 10(p-1)(q-1)$$

Alors $d = -2047 \pmod{(p-1)(q-1)} = 1433$.

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

a. Trouvez k tel que $b = a^k$.

Solution. La liste de puissances de 2 mod p sont :

k	0	1	2	3	4	5	6	7	8	9	10
2^k	1	2	4	8	16	32	5	10	20	40	21
k	11	12	3	14	15	16	17	18	19	20	21
2^k	42	25	50	41	23	46	33	7	14	28	56

qui demontre que $56 = 2^{21} \pmod{p}$, alors $k = 21$.

Remarque : En général il faut construire en moyenne une liste de $(p-1)/2$ puissances pour trouver k . Quand p est plus grand, il est mieux de construire deux listes de longueur $m = \lfloor \sqrt{p-1} \rfloor$:

i	0	1	2	3	4	5	6	7
2^i	1	2	4	8	16	32	5	10
j	0	1	2	3	4	5	6	
$56 \cdot 20^j$	56	29	54	9	31	15	32	

pour trouver un identité $a^i \pmod{p} = ba^{mj} \pmod{p}$ et alors

$$k = (i - mj) \pmod{p-1}.$$

Dans cet exemple, l'identité $32 = 2^5 \pmod{59} = (56 \cdot 2^{7 \cdot 6}) \pmod{59}$ implique

$$k = (5 - 42) \pmod{58} = -37 \pmod{58} = 58 - 37 = 21.$$

b. Calculez un chiffrement de $m = 7$ avec la clé publique ElGamal (p, a, b) . Pourquoi n'est-t-il pas unique ?

Solution. Le chiffrement nécessite un choix de exposant ℓ , alors pour $10 \leq \ell \leq 12$, on trouve des possibles chiffrements (r, s) :

ℓ	a^ℓ	b^ℓ	mb^ℓ	(r, s)
10	21	49	48	(21, 48)
11	42	30	33	(42, 30)
12	25	28	19	(25, 19)

c. Montrez les étapes pour déchiffrement de votre texte chiffré.

Solution. Pour un texte chiffré (r, s) il faut (1) trouver $r^{-1} \bmod p$, (2) calculer sa puissance $r^{-k} \bmod p$, et (3) prendre le produit $m = r^{-k}s \bmod p$. Le premier étape peut être calculer avec un pgcd étendu ; si on a

$$ur + vp = 1,$$

alors $r^{-1} \bmod p = u \bmod p$. Pour les chiffrements au-dessus, ces résultats se trouvent dans le tableau suivant :

(r, s)	r^{-1}	r^{-k}	$r^{-k}s$
(21, 48)	45	53	7
(42, 30)	52	2	7
(25, 19)	26	19	7