Exercice RSA

On considère les valeurs **p= 3**,**q= 11** et **e= 3**.
• Calculez la valeur publique **n**.
• Calculez la fonction d'Euler **φ(n)**.
• Utilisez l'algorithme étendu d'Euclide pour calculer la valeur de la clé privée **d**.
• Chiffrez le message **m=5**.
• Déchiffrez le message **c=26**.

Solution

n = p*q = 3 * 11 = **33**
φ(n) = (p-1) * (q-1) = 2 * 10 = **20**
e = 3 < 20 et PGCD(3, 20) = 1

$d = 3^{-1} \% 20$
20 = 6*3 + 2
3 = 1*2 + 1
1 = 3 – 1*2
1 = 3 – (20-6*3)
1 = 3 – 20 + 6*3
1 = -20 + 7*3
d=7

chiffrement: m=5 → c= 5^3 % 33 = **26**
déchiffrement: c=26 → m=26^7 % 33 = **5**