Sécurité Informatique
Interrogation 2

Exercice

Alice construit un cryptosystème RSA à partir des deux nombres **p = 7** et **q = 11**.

1. Quel exposant **e** faut-elle choisir entre ces valeurs : **6, 7, 71** ? Justifiez pour chaque valeur.
   n = p * q = 77, φ(n) = 60.
   e ≠ 6 – PGCD (6, 60) ≠ 1 . (0.5 pts)
   e = 7 – PGCD (7, 60) = 1 et 1 < 7 < 60. (0.5 pts)
   e ≠ 71 – 1 < 71 < 60 . (0.5 pts)
2. Quelle est la clé publique ?
   Clé publique = (7, 77). (0.5 pts)
3. Trouvez les coefficients de Bézout (u et v).
   e * u + φ(n) * v = 1 (0.5 pts)
   60 = 7 * 8 + 4 …… (1)
   7 = 4 * 1 + 3 …… (2)
   4 = 3 * 1 + 1 …… (3)
   1 = 4 – 3 * 1
   1 = 4 – 7 + 4
   1 = - 7 + 2 * 4
   1 = -7 + 2 * (60 – 7 * 8)
   1 = -7 + 2 * 60 – 7 * 16
   1 = 2 * 60 – 7 * 17
   u = - 17, v = 2 ou bien u = -17 mod 60 = 43, v = 2 (1 pts)
4. Donnez la clé privée.
   Clé privée = (43, 77). (0.5 pts)
5. Donnez la fonction de chiffrement, puis chiffrez le message **M = 3**.
   $C = M^e \bmod n$ (0.5 pts)
   $C = 3^7 \bmod 77 = 31$ (0.5 pts)
6. Donnez la fonction de déchiffrement, puis déchiffrez le message **C = 2**.
   $M = C^d \bmod n$ (0.5 pts)
   $M = 2^{43} \bmod 77 = 30$ (0.5 pts)