D13 : arithmétique

25 juin 2013

L'objecif de l'exercice est de décchiffrer le message hexadécimal :

$$C2 - 24 - C2$$

sachant que le système RSA de module $n = 253$ a été utilisé avec un exposant de chiffrement $e = 17$. On utilise les notations habituelles i.e. d, e, ϕ, n, p, q.

1. Convertir les nombres 0x$C2$ et 0x24 en décimal.
2. Déterminer les premiers p et q.
3. Calculer ϕ.
4. Déterminer d tel que $ed = 1 \pmod{\phi}$.
5. Décrypter les entiers de la question [a].
6. Décoder le message.