D13 : arithmétique

25 juin 2013

L'objectif de l'exercice est de déchiffrer 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.

$$0xC2 = 194, \quad 0x24 = 36$$

2. Déterminer les premiers p et q. Le module est divisible par 11,

$$n = 11 \times 23$$

3. Calculer ϕ.

$$\phi = 10 * 22 = 220$$

4. Déterminer d tel que $ed = 1 \pmod{\phi}$.
   On applique l'algorithme du cours.

1	0	220
0	1	17
1	-12	16
-1	13	1

   D'où $-220 + 13 \times 17 = 1$, et donc $d \equiv 13$.

5. Décrypter les entiers de la question [a].

$$D(194) \equiv 194^d \equiv 222, \quad D(36) \equiv 36^d \equiv 192.$$

6. Décoder le message.

$$222 = 0xDE, \quad 192 = 0xC0$$

   Le message est : DE-C0-DE.