D13 : arithmétique

10 janvier 2013

On considère les entiers $p = 89$, $q = 97$ et on note $n = pq$.

1. p et q sont-ils premiers ? Oui. Il suffit de tester la divisibilté de p par les entiers premiers inférieurs à 9. Or p n'est pas disvisible par 2, 3, 5, et 7. Idem pour q.
2. Déterminer des entiers u et v tels $89u + 97v = 1$. On applique l'algorithme d'euclide étendu du cours qui consiste à combiner les relations linéaires (x, y, z) satisfaisant $x97 + y89 = z$:

1	0	97
0	1	89
1	-1	8
-11	12	1

   D'où la solution : $u = 12$ et $v = -11$.
3. Résoudre $x^2 = 1$ modulo n. D'aprés le cours, comme n est produit de deux premiers distincts, il y a quatre solutions correspondants aux solutions $(\pm 1, \pm 1)$ par le thèorème chinois des restes.

   Une solution non triviale est donnée par

   $$-11 * 89 * (-1) + 12 * 97 * 1 = 2135$$

   les autres solutions sont : 1, -1 et -2135.
4. Calculer $\phi(n)$. La fonction est multiplicative,

   $$\phi(n) = (p - 1) * (q - 1) = 96 * 88 = 8448$$

5. Pour RSA, quelle est la clef secrète associée à l'exposant publique $e = 5$? Il faut résoudre Bâchet-Bézout pour 8448 et 5 :

1	0	8448
0	1	5
1	-1689	3
-1	1690	2
2	-3379	1

   La clef secrète vaut :

   $$d = 5069.$$

6. Calculer le chiffré de $x = 2$. C'est tout simplement 32. Le déchiffrement de 2 aurait été un peu plus long à obtenir.