D13 : arithmétique

5 janvier 2015

On considère les entiers $p = 89$, $q = 179$. Dans la suite, vous utiliserez librement le résultat des commandes suivantes :

```
exam> p=89
exam> let q=2*p+1
exam> factor $q
179: 179
exam> bc <<< "(2^$p) % $q"
178
```

1 exercice

1. p et q sont-ils premiers ?
2. Que peut-on dire de plus sur p et q ?
3. Quel est l'ordre de 2 modulo q ?

2 exercice

Calculer les paramètres du système de chiffrement RSA de module $n = pq$ correspondant à l'exposant de chiffrement $e = 5$.

3 exercice

Utiliser la méthode dite "pas de bébé, pas de géant" pour calculer le logarithme discret de 3 en base 2. Prendre soin de détailler les principales étapes de l'algorithme.