Exercices Série 10

1. Appliquez le chiffrement et déchiffrement du nombre m = 49 avec les données suivantes : $p = 11, q = 23 \; et \; e = 21$.

2. Montrez que si $p, q \in \mathbb{N}^*$ sont des nombres premiers, alors $\varphi(p \times q) = (p-1) \times (q-1)$.

Facultatifs

3. Appliquez le chiffrement avec le nombre de César égal à 11 pour le mot « bonjour ».

4. Appliquez l'algorithme modulo 10 récursif utilisé sur les BVR pour la séquence 159785.

Corrigé :

1. $n = 253$, $\varphi(n) = 10 \times 22 = 220$ et par Euclide étendu on obtient $1 = 220 \times (-2) + 21 \times 21$, donc la clé privée est $d = 21$.
   Note : ici, c'est un hasard que $e = d$!!!
   Les message chiffre est $\mu = 49^{21} mod\ 253 = 192$. Et pour déchiffrer, on vérifie que $m = 192^{21}\ mod\ 253 = 49$, qui est bien le message de départ !

2. Notons d'abord qu'il y a au total $p \times q$ nombres entre 1 et $p \times q$. Donc la valeur maximale de $\varphi(p \times q\ )$ est $p \times q$ si on les compte tous. Procédeons par élimination et supprimons de la liste des $p \times q$ candidats tous ceux qui ne sont PAS premiers avec $p \times q$.
   Etant donné que p et =q sont des nombres entiers, $p \times q$ n'a que 4 diviseurs $(1, p, q, p \times q)$.
   Ainsi, les nombres n'étant PAS premiers avec $p \times q$ ont au moins un facteur commun parmi $p, q, p \times q$. Or comme nous nous intéressons aux nombres compris entre 1 et $p \times q$, le facteur commun est forcément p ou q (seul $p \times q$ est divisible par $p \times q$) !
   Les facteurs NON-premiers avec $p \times q$ sont donc tous les multiples de p ET tous les multiples de q. Il y a au total p multiples de q entre 1 et $p \times q$ $(1q, 2q, 3q, \dots, (p-1) \times q$ et $p \times q)$.
   De même, il y a q multiples de p entre 1 et $p \times q$.
   Donc, on dénombre $p + q$ nombres qui ne sont PAS premiers avec $p \times q$. Toutefois, on note que $p \times q$ est compté 2 fois (comme multiple de p ET comme multiple de q). Ce qui donne donc $p + q - 1$ nombres différents qui ne sont pas premiers avec $p \times q$ entre 1 et $p \times q$.
   Donc $\varphi(p \times q\ ) = p \times q - p - q + 1 = (p-1) \times (q-1)$.

   CQFD.

3. On décale chaque lettre de 11 positions (a devient p, b devient q, …)
   Le résultat est donc « qdcydjg ».

4. En appliquant la méthode on obtient 2.