# Sécurité Informatique
## Interrogation 1

### Exercice

Soit l'anneau $Z_{30}$ (alphabet à 30 caractères), on représente les caractères avec des entiers selon le tableau suivant :

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | . | , | - | : |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |

Le chiffrement multiplicatif consiste à multiplier toutes les lettres du texte en clair **M** par une lettre fixé qui sert de clé **K**. On définit la fonction de chiffrement multiplicatif par :

**E (M) = M*K mod 30.**

1. Trouver tous les éléments inversibles de cet alphabet.
   Les éléments inversibles sont les éléments X tel que : PGCD(X,30) = 1.
   Les éléments inversibles sont : B, H, L N, R, T, X, : ou 1, 7, 11, 13, 17, 19, 23, 29 (1 pts)
2. Quel sont les clés possibles pour le chiffrement ?
   Les clés possibles sont tous les éléments inversibles sauf 1. (0.5 pts)
3. Calculer la clé inverse de 13.
   La clé inverse de 13 est $\mathbf{K^{-1}}$ **=**7 car : 13 * 7 mod 30 = 1. (1 pts)
4. Trouver la fonction de déchiffrement **D (C)**.

   **D (C) = C*$K^{-1}$ mod 30.** (0.5 pts)

5. Chiffrer le texte « **AVRIL** » avec la clé 13.

| | | |
|---|---|---|
| M = A : 00 | Chiffrement : (00 * 13) mod 30 = 00 | C = A. |
| M = V : 21 | Chiffrement : (21 * 13) mod 30 = 03 | C = D. |
| M = R : 17 | Chiffrement : (17 * 13) mod 30 = 11 | C = L. |
| M = I : 08 | Chiffrement : (08 * 13) mod 30 = 14 | C = O. |
| M = L : 11 | Chiffrement : (11 * 13) mod 30 = 23 | C = X. |

**C = ADLOX** (1.5 pts)

6. Déchiffrer le texte « **GWL.O** » qui a été chiffré avec la clé 13.

| | | |
|---|---|---|
| C = G : 06 | Déchiffrement : (06 * 7) mod 30 = 12 | M = M. |
| C = W : 22 | Déchiffrement : (22 * 7) mod 30 = 04 | M = E. |
| C = L : 11 | Déchiffrement : (11 * 7) mod 30 = 17 | M = R. |
| C = . : 26 | Déchiffrement : (26 * 7) mod 30 = 02 | M = C. |
| C = O : 14 | Déchiffrement : (14 * 7) mod 30 = 08 | M = I. |

**M = MERCI** (1.5 pts)