

## **Rapport du travail pratique: Polynômes et Reed-Solomon**

Lors de la réalisation de ce travail pratique, nous avons pu mettre en place les connaissances théoriques acquises pendant les cours. De ce fait, nous avons implémenté les théorèmes et algorithmes suivants :

- Théorème de LaGrange
- Théorème de Bachet-Bézout
- Algorithme d'Euclide étendu
- Algorithme de l'inverse modulaire
- Algorithme de l'évaluation de polynômes

Afin de décrypter le message de base nous avons procédé comme suit:

Dans un premier temps, nous avons converti notre liste initiale en une liste de points depuis le 24<sup>ème</sup> indice dans le but de stocker les 19 derniers points de notre liste initiale qui correspondent aux points corrects. De plus, nous avons généré deux paires de points uniques situés entre l'indice 0 et 23 pour par la suite évoluer les bons polynômes qui passent parmi les 32 points.

Pour chaque nouveau polynôme, on applique le théorème de Lagrange pour qui nous retourne une liste à évaluer. Si le nombre de points de notre liste précédemment testée par Lagrange passent par 32 points de notre liste initiale, nous pouvons affirmer que c'est le bon polynôme.

Pour finir, une fois  $L(x)$  trouvé, nous avons pris chacun des points de notre liste « juste » pour les évaluer afin de retrouver les valeurs de la liste originale. Ces valeurs sont retournées sous la forme d'entier et nous avons dû les convertir en texte à l'aide de la fonction « chr » (ASCII).

Résultat obtenu :

**« Ce secret est minable »**

En conclusion, la difficulté de ce travail pratique se résume en l'application de concepts mathématiques en programmation. Malgré le fait que python soit un langage de programmation "permissif" et de haut niveau, l'algorithme des différentes fonctions implémentées peut s'avérer plus compliqué. Prenons l'exemple de la fonction d'Euclide étendu. Elle utilise la récursivité pour calculer les pgcd et les coefficients de Bachet-Bezout. Nous avons éprouvé des difficultés à adapter un concept vu dans les cours de mathématiques en technologie de l'information et appliquées.