Choix implémentation

Pour l'implémentation j'ai premièrement choisi de passer par le type primitif du langage c en regardant leurs tailles et je les ai renomés avec la lettre i pour les variables signées et u pour les non signées. Je n'ai besoin que d'entiers sur 24 bits, que je stockerai sur 32 bits (taille d'un `int`) et d'entiers sur 80 bits que je stockerai dans une structure, un tableau de 10 `char` (stocké sur 1 octect).

De plus j'ai ajouté une structure `msgCLe_t` pour avoir l'association entre un message, chiffré ou non et sa clé. Ainsi la liste chiffré et la liste clair seront de type `msgCle_t`.

Enfin j'ai rempli à la main les tableaux inverses des tableaux de substitution et de permutation afin de ne pas les parcourir pour trouver la position de l'élément `x` cela rend le code plus rapide mais prend un peu plus de mémoire.

voici le résultat :

Tableau substitution inversé : S[x] = {5, 14, 15, 8, 12, 1, 2, 13, 11, 4, 6, 3, 0, 7, 9, 10}

Tableau permutation inversé : P[x] = {0, 4, 8, 12, 16, 20, 1, 5, 9, 13, 17, 21, 2, 6, 10, 14, 18, 22, 3, 7, 11, 15, 19, 23}

Attaque par le milieu

Pour l'attaque par le milieu j'ai appliqué la méthode suivante :

Remplissage de la liste clair avec toutes les clés possibles sur 2^24 bits, et triage par ordre croissant.

Remplissage de la liste chiffre avec toutes les clés possibles sur 2^24 bits, et triage par ordre croissant.

Recherche des collisions en appliquant l'algorithme `rechercheDichotomique` sur la liste clair pour chaque élément de la liste chiffré.

Dans cette recherche je regarde si j'ai trouvé une collision, si oui :

Je regarde dans la liste clair si ce message est dupliqué mais avec des clés différentes.

Je regarde au dessus et en dessous de ce dernier puisque la liste est triée.

Pour chaque messages similaires je test si les clé sont correctes. Afin d'y parvenir je chiffre un message, issue d'un autre couple de clair-chiffre, avec la clé de l'élément dans la liste clair, puis je chiffre ce résultat avec la clé issue de la liste chiffre. Enfin je vérifié que cela me donne le chiffre du couple clair-chiffré. Si tel est le cas je peux afficher le couples de clés.