Les Sujets

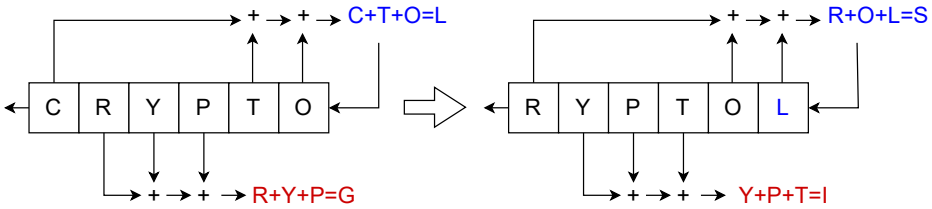
Chiffrement LFSR filtré

On propose la méthode qui permet de chiffrer des mots de la manière suivante.

- on considère un mot de passe secret composé de 6 lettres, par exemple $code = CRYPTO$.
- on veut chiffrer un mot, par exemple MESSAGE
- on considère les 2e, 3e et 4e lettres du code (CTO), qu'on va "ajouter" à la première lettre du mot à chiffrer (M). On obtient $R + Y + P + M = 18 + 25 + 16 + 13 = 72$ qu'on prend modulo 26, donc 20, c'est à dire la lettre "T".
- la 2e lettre du mot est chiffrée par les lettres 3, 4 et 5 du mot de passe.
- la 3e lettre du mot est chiffrée par les lettres 4, 5 et 6 du mot de passe.
- à partir de la 4e lettre du mot, on doit créer des lettres supplémentaires du mot de passe. Ces lettres sont créées de la manière suivante : la lettre 7 est la somme des lettres 1, 5 et 6 du mot de passe. La lettre 8 est la somme les lettres 2, 6 et 7 et ainsi de suite.

Les Sujets

Chiffrement LFSR filtré



Clé = CRYPTO

M	E	S	S	A	G	E
+	+					
G	I	· · · · ·				
=	=					
T	N	· · · · ·				

Les Sujets

Chiffrement LFSR filtré

Tester l'algorithme

Chiffrez et déchiffrez (en connaissant les 6 lettres de la clé de chiffrement) le mot MATHEMATIQUES.

Cassez l'algorithme

Maintenant, vous ne connaissez pas la clé de chiffrement. Proposez un algorithme pour déchiffrer n'importe quel message. (on vous fournira un message à cassser)

Améliorez l'algorithme

Proposez des améliorations de l'algorithme, qui se basera toujours sur une combinaison de 3 lettres d'une clé à 6 lettres, mais avec une autre manière de les combiner (ici on les ajoute, mais on pourrait faire autrement). Est-ce que ça va rendre l'algorithme plus robuste ?