Cryptographie et théorie des nombres

Zakaria RIDADARAJAT

02/02/2021

Synthèse

Github: **https://github.com/ARSICMrk/ARSIC_PSBx/tree/main/Maths_BD/Cryptographie**

Le document évalué dans le cadre de ce rendu a été produit par William ROBACHE et Marko ARSIC sur la cryptographie et la théorie des nombres.

La cryptographie désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Le but derrière ces techniques est d'assurer la confidentialité des messages entre deux interlocuteurs. Les auteurs du rapport commencent par présenter la différence entre le cryptage classique et le cryptage a clé symétrique et nous montre les limites de chacune, et ils nous introduisent aussi les différents concepts mathématiques qui sont appliqué à la science de la cryptologie.

Explication des formules

$f_D(M) = f_D\left[f_C(m)\right] = m$

La formule ci-dessus résume le principe chiffrement qui rendre la compréhension d'un message tangible pour le récepteur. Les auteurs expliquent ce principe d'une manière clair, en effet pour envoyer un message m toute en réduisant le risque qu'une personne tombe dessus, on a besoin de deux fonctions f_C et f_D La fonction f_C permet de camoufler le message autrement dit de le chiffrer et dès que le récepteur rereçoit le message il pourra déchiffrer le message grâce à la fonction f_D.

Evaluation

1) lisibilité du rapport :

Il est très agréable sur le plan visuel.

2) qualité du rapport :

Ils sont présentés un document sont sommaire, ni section

3) Aspect didactique

La lecture de ce dossier est accessible. Elle ne nécessite pas un niveau mathématique très élevé.

4) Bibliographie :

Effectivement, les auteurs ont mentionné la bibliographie à la fin du rapport pour les gens qui veulent approfondir un peu plus sur le sujet.

5) Qualité du LaTeX

Les équations sont relativement simples, de qualité et maitrisées.

Conclusion :

A mon sens, il s'agit d'un bon travail. Les auteurs fournissent un dossier recherché, documenté et globalement facile à lire. Ce document apporte des notions simplistes pour découvrir le monde de la cryptographie.

Personnellement, j'apprécie beaucoup la façon donc les notions mathématiques ont été explicités.