

Evaluation des dossiers sur les mathématiques du Big Data

Les « 12 travaux d'AstéRix »

Daif Hakim

27/01/2021

Cryptographie et théorie des nombre

1. Critères d'évaluation

Dans ce dossier, nous allons parcourir et faire une évaluation des travaux de mes camarades en mathématiques du Big Data:

Nos critères seront :

1. Visuel et l'organisation du dossier: Es ce que la mise en page est propre, agréable à lire ou non ? Le travail est-il organisé (chapitres, sections, sous-sections, Parties)

2. Qualité du latex et des formules mathématiques : Es ce que les formules sont claires ou pas ? Es ce que le dossier contient le code Latex ou le rapport sous format Rmd ? **3. Compréhension de l'idée générale:** Les Auteurs arrivent-ils à transmettre l'idée générale ?

4. Explication et compréhension des formules mathématique et des concepts fondamentaux: Es ce que les formules et les notions sont bien expliquées ?

5. Difficulté et originalité du thème : Le sujet abordé est-il original/difficile ou pas ? ## 2. Lien vers le document commenté

Le document évalué dans le cadre de ce rendu a été fait par ARSIC Marko et ROBACHE William sur l'analyse des Cryptographie et théorie des nombre.

lien vers leur Github: <https://github.com/WilliamRbc/PSBX/blob/main/CRYPTO/Cryptographie.pdf>

le dossier en question est **Cryptographie.pdf**

3. Synthèse de la présentation

La cryptographie est la science qui cherche à fabriquer des codes secrets, à trouver le code de messages secrets. Aujourd'hui, grâce aux performances de plus en plus élevées des ordinateurs, elle intervient dans tous les domaines de la sécurité militaire mais aussi civile. elle désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique. Elle est notamment utilisée pour garantir la confidentialité des échanges sur Internet, pour protéger des données sensibles dans les entreprises, pour garantir l'identité des parties contractantes en introduisant des protocoles de signature en particulier sur Internet.

ARSIC Marko et ROBACHE William vont s'intéresser plus précisément sur deux types de cryptographie: La cryptographie symétrique et La cryptographie asymétrique.

Les auteurs, en gros, ils ont fait une comparaison entre les deux types de cryptologie et cela en montrant les limites de chacune, et exposant les différents concepts mathématiques qui sont appliqué à cette science.

Après lecture de ce document on peut voir clairement que la différence fondamentale qui distingue le cryptage symétrique et asymétrique est que le cryptage symétrique permet le cryptage et le décryptage du message avec la même clé. Tandis que, le cryptage asymétrique utilise la clé publique pour le chiffrement et une clé privée pour le déchiffrement.

Explication des formules

$$f_D(M) = f_D[f_C(m)] = m$$

La formule ci-dessus résume le principe de chiffrement qui rend la compréhension d'un message tangible pour le récepteur. Les auteurs expliquent ce principe d'une manière claire, en effet pour envoyer un message m tout 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 reçoit le message il pourra déchiffrer le message grâce à la fonction f_D .

5. Evaluation

1. Visuel et l'organisation du dossier: Le visuel est agréable, travail très organisé (section, titres, exemples) cependant on constate que l'enchaînement des idées n'est pas clair, on sent que les sections et les sous-sections n'ont aucune relation, manque d'éléments et des expressions de transitions.

2. Qualité du latex et des formules mathématiques : il n'y a pas assez de formules mathématiques, donc on ne peut pas vraiment juger la qualité des formules utilisées ni la maîtrise du code latex.

3. Compréhension de l'idée générale : Après une première lecture on comprend très bien chaque partie, vu que les expressions utilisées sont d'une simplicité remarquable, cependant comme on l'a indiqué précédemment, l'enchaînement des idées (entre section et sous-section) n'est pas très bien clair et cela nous empêche de comprendre facilement l'idée générale.

4. Explication et compréhension des formules mathématiques et des concepts fondamentaux: malheureusement on ne trouve pas des formules mathématiques et pas de concepts mathématiques, ce qui rend l'évaluation à la base de ce critère casé impossible.

*5. Difficulté et originalité du thème : ** le sujet abordé est très original, en termes de difficultés, c'est un sujet assez difficile si les auteurs ont entré dans les détails.

6. Conclusion

En conclusion, on trouve que le sujet est très intéressant et original, très facile à lire, des expressions très claires, la compréhension des parties séparément est assurée, j'apprécie trop le fait qu'ils ont choisi un tel thème, cependant ils auraient pu faire beaucoup mieux en touchant plus aux aspects mathématiques notamment en utilisant des formules et des théorèmes mathématiques.