25614 AZZOUZI Hamza

Techniques de cryptographie

La cryptographie est devenue l'une des problématiques les plus importantes ces dernières années. Ce sujet montre l'interaction entre les domaines abstraits des mathématiques et les enjeux les plus importants. En effets l'algèbre moderne a été utilisée pour trouver des moyens sécurisés afin de protéger les différentes données numériques.
La cryptographie est utilisée dans différents domaines afin d'assurer essentiellement la protection des données. De plus la cryptographie est largement utilisée dans le domaine de la télé-médecine pour protéger les informations personnelles des patients.

Positionnement thématique (ETAPE 1)

MATHEMATIQUES (Algèbre), INFORMATIQUE (Informatique pratique).

Mots-clés (ETAPE 1)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Cryptographie	*Cryptography*
Méthode César	*Cesar Method*
RSA	*RSA*
Test de primalité	*Primarity test*
Logarithme Discret	*Discret Logarithm*

Bibliographie commentée

La protection des données a depuis longtemps été une majeure problématique. D'innombrables techniques ont été utilisées pour l'unique raison de protéger les données. La méthode César(ou chiffrement par décalage) est la première technique de cryptographie utilisée[3]. Cette technique consiste à réaliser un décalage des lettres de l'alphabet(César faisait un décalage de trois lettres par exemple). De nombreuses techniques ont ensuite été créées s'inspirant du chiffrement par décalage[1]. Cependant toutes ces techniques peuvent être déchiffrer grace à des codes informatiques.
En 1976,Whitfield Diffie et Martin E. Hellman publièrent leur article : *New Directions in Cryptography* [1]dans lequel ils présentèrent le principe de la cryptographie à clé publique(ou asymétrique). Ce procédé consiste à utiliser une clé publique qui cherche à chiffrer les informations et qui est facile à coder et une clé privée qui sert à déchiffrer dont le décodage est impossible. L'exemple le plus concret des chiffrement asymétriques est le chiffrement RSA [1]
dont le nom vient des trois chercheurs ayant trouvé cette méthode *Ronald Rivest, Adi Shamir et Leonard Adleman*. Cette méthode utilise les propriétés arithmétiques des nombres premiers afin de chiffrer et de déchiffrer les données. Il est largement utilisé dans les entreprises pour les signatures numériques ainsi que les chiffrements.
La méthode RSA nécessite la connaissance des grands nombres premiers. Pour cela plusieurs tests de primalité ont été développés afin d'assurer la non primalité d'un nombre premier[5]. Les tests de Fermats ainsi que ceux de Miller-Rabin[6] sont des exemples de tests de primalités probabilistes.

L'arithmétique des nombres est largement utilisé dans le domaine de la cryptographie. On s'appuie par exemple sur le problème du logarithme discret comme outil de cryptographie. Dans l'article *New Directions in Cryptography* de Diffie-Helmann[2], les deux chercheurs introduisent l'idée de la clé publique. Ils montrent l'échange d'une clé appelée clé de Diffie-Helmann. Une autre technique de cryptographie largement utilisée est la technique d'Elgamal qui s'appuient sur la difficulté du problème de Diffie-Helmann ainsi que celui du logarithme discret pour sécuriser les échanges des informations.

Problématique retenue

Il s'agit de savoir dans quelle mesure la cryptographie permet-elle de sécuriser les informations utilisées en télé-médecine.

Objectifs du TIPE

Je vais essayer de :
Etudier les premières techniques de cryptographie ainsi d'essayer de les programmer.
Etudier quelques propriétés arithmétiques des nombres. premiers qui permettent de réaliser la technique RSA.
Programmer quelques test de primalité.
Etudier le problème du logarithme discret et quelques techniques de chiffrage qui en découlent.

Références bibliographiques (ETAPE 1)

[1] Jeffrey Hoffstein : An introduction to mathematical cryptography
[2] Whitfield Diffie and Martin E. Hellman : New Directions in Cryptography :
https://www.cs.utexas.edu/~shmat/courses/cs380s_fall08/dh.pdf
[3] cours de cryptographie à l'université de Lille : *http://math.univ-lille1.fr/~bodin/fichiers/ch_crypto.pdf*
[4] Evan Dummit : Cryptography (part 3): Discrete Logarithms in Cryptography
[5] Pierre Rouchon : Arithmétique et Tests de Primalité :
https://studylibfr.com/doc/658008/arithm%C3%A9tique-et-tests-de-primalit%C3%A6
[6] Keith Conrad : The Miller Rabin Test :
https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf

DOT

[1] *Septembre : choix du sujet et premières études documentaire*
[2] *Octobre : compréhension et détermination des principales techniques à présenter*
[3] *Janvier : Lecture et compréhension des cours sur les tests de primalité*
[4] *Février : implémentation des tests de primalité*
[5] *Mai : Finalisation de la présentation*