TIPE :
Cryptographie symétrique AES - Protéger des données de santé

Ancrage au thème de l'année : (max 50 mots)
La santé d'une personne peut être représentée par beaucoup de données numériques. Nous allons nous intéresser à la protection de celles ci à l'aide d'un système de chiffrement d'informations, afin de prévenir la fuite de ces données sensibles.

Motivation du choix : (max 50 mots)
Passionné par l'informatique et les algorithmes un peu complexe, j'étais très intrigué par le fonctionnement d'un algorithme de cryptographie comme celui choisi ici (AES), ainsi que tout l'algèbre permettant son fonctionnement, et j'ai adoré en faire ma propre implémentation.

Professeurs encadrant :
A. JOSEPH, A. DELEPINE, D. HARRIVEL, L. JACQUET-MALO

Positionnement thématique :
INFORMATIQUE (Informatique Théorique: Cryptographie)
MATHÉMATIQUES (Algèbre: Arithmétique, Structures algébriques, Algèbre linéaire, Codages par corps finis)

Mots clés :

Mots clés en français	Mots clés en anglais
Données de santé	Health data
Protection de données	Data protection
Chiffrement symétrique AES	AES Symmetric encryption
Algorithme	Algorithm
Matrice à coefficients dans un corps fini	Matrix with elements from a Galois field

Bibliographie commentée : (max 650 mots)
Nous possédons tous des données concernant notre santé, comme notre groupe sanguin, notre taille et notre poids, etc… Certaines d'entre elles sont amenées à être stockées numériquement sur des appareils, comme par exemple une montre connectée pourrait prélever notre rythme cardiaque à intervalle régulier, afin de prévenir une quelconque anomalie cardiaque. Ces données sont des données sensibles, et nécessitent d'être stockées de manière sécurisée. Afin de sécuriser ces données, nous allons nous pencher sur la cryptographie.
La cryptographie est un système de chiffrement de l'information, dans l'objectif de sécuriser des données. Elle utilise un système de clé, afin de permettre que la lecture des données soit possible uniquement si l'on possède la clé qui a chiffré les données. Nous avons choisi d'étudier le système de chiffrement symétrique AES (Advanced Encryption Standard).
En 1997, le NIST a lancé un appel à propositions pour un nouveau système de chiffrement, car les systèmes utilisés avant, comme le DES ou le 3DES n'étaient pas assez sécurisé, ou trop lent. Le NIST et la communauté scientifique internationale ont discuté des avantages et des inconvénients des chiffrements soumis et ont réduit au fur et à mesure le nombre de candidats. Finalement, en 2001, le NIST a déclaré le chiffrement par bloc Rijndael comme le nouvel AES et l'a publié en tant que norme finale [1]. Le chiffrement AES est tellement efficace qu'il est devenu obligatoire dans plusieurs normes industrielles et est utilisé dans plusieurs systèmes commerciaux (sécurité internet, cryptage Wi-Fi, réseau Skype, etc…). D'ailleurs il a été approuvé par le gouvernement fédéral américain, et la NSA (National Security Agency) des Etats-unis a annoncé qu'elle autorisait l'AES à chiffrer les documents classifiés.
Nous allons donc nous centrer sur la manière dont les données sont chiffrées par l'algorithme AES. En nous penchant sur l'œuvre de Christof Paar et Jan Pelzl [2], nous allons étudier les structures algébriques nécessaire à la compréhension de l'algorithme, à savoir les matrices à coefficients dans un corps fini de caractéristique 2 et de cardinal 256, puis le cœur de l'algorithme par ses différentes étapes, et ses différents ciphers. Afin de visualiser les différents ciphers de l'algorithme, nous allons appliquer le chiffrement sur des images, ce qui nous mène à étudier la structure du format d'image PNG [3] ainsi que son format de compression DEFLATE [4]. Enfin, nous appliquerons notre implémentation de l'algorithme sur des données de santé, extraites au préalable de données d'exercice physique d'une Apple Watch grâce au framework HealthKit [5], afin de montrer que nous pouvons les protéger.

TIPE :
Cryptographie symétrique AES - Protéger des données de santé

Problématique retenue : (max 50 mots)
Il est ici question de protéger des données de santé de patients à l'aide de l'algorithme de chiffrement symétrique AES, et de comparer l'efficacité des différents ciphers sur ces données.

Objectif du TIPE : (max 100 mots)
Dans ce TIPE, les objectifs sont de :
- Etudier les structures algébriques requises (Matrices et arithmétique dans un corps finis)
- Comprendre et implémenter l'algorithme de chiffrement AES
- Appliquer cet algorithme sur une image afin de visualiser l'efficacité des ciphers
- Protéger des données réelles de santé en utilisant l'algorithme

Références bibliographiques : (2 à 10 références)
[1] Wikipédia: Advanced Encryption Standart. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[2] Christof Paar, Jan Pelzl : *Understanding Cryptography*. Springer. 2009.
[3] W3C : Portable Network Graphics (PNG) Specification (Second Edition) https://www.w3.org/TR/PNG/
[4] Marin Moulinier : DEFLATE : L'algorithme que vous retrouvez partout. 2020. https://compression.fiches-horaires.net/la-compression-sans-perte/deflate-lalgorithme-que-vous-retrouvez-partout/
[5] Apple: Health and Fitness - Apple developer. https://developer.apple.com/health-fitness/