36651 FALLET Nathan

Cryptographie symétrique AES : Protéger des données de santé

Passionné par l'informatique et les algorithmes complexes, j'étais très intrigué par le fonctionnement d'un algorithme de cryptographie comme celui choisi ici (AES), ainsi que par l'algèbre sous-jacente, et j'ai apprécié en faire ma propre implémentation.
L'analyse de la santé d'une personne est associée à de nombreuses données numériques. Cela va du dossier médical partagé aux mesures des montres connectées. Nous allons nous intéresser à la protection de celles-ci à l'aide d'un système de chiffrement d'informations, afin de prévenir leur fuite.

Positionnement thématique (ETAPE 1)

INFORMATIQUE (Informatique Théorique), MATHEMATIQUES (Algèbre), INFORMATIQUE (Informatique pratique).

Mots-clés (ETAPE 1)

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

Nous possédons de plus en plus de données associées à notre santé, comme notre activité physique, notre groupe sanguin, notre poids, ou encore l'historique de nos récentes maladies. Ces données permettent l'analyse de notre santé afin d'obtenir un suivi et une prise en charge adaptée. Certaines d'entre elles sont amenées à être stockées numériquement, dans notre dossier médical partagé, ou dans des objets connectés, comme par exemple une montre connectée qui enregistre 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, ce qui est possible grâce à la cryptographie.

La cryptographie est un système de chiffrement de l'information, basé sur l'utilisation de clés. Il en existe différents systèmes : ceux dits symétriques, qui utilisent la même clé pour le chiffrement et le déchiffrement, et ceux dits asymétriques, qui utilisent une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Le DES et le 3DES étaient les principaux systèmes de chiffrement symétriques, jusqu'à ce qu'en 1997 le NIST (National Institute of Standards and Technology) lance un appel à propositions pour un nouveau système de chiffrement pour les remplacer, ceux-ci étant devenus trop lents et insuffisamment sécurisés. Finalement, en 2001, le NIST a déclaré le chiffrement par bloc Rijndael (créé par Vincent Rijmen et Joan Daemen) comme le nouvel AES

(Advanced Encryption Standard) 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 de nombreuses technologies (HTTPS, Wi-Fi, Skype, NSA, ...).

Nous allons nous centrer sur le fonctionnement de l'algorithme AES, en étudiant tout d'abord les structures algébriques nécessaires 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 modes de fonctionnement, comme expliqué dans le livre de Christof Paar et Jan Pelzl [2]. Afin d'illustrer l'efficacité des différents modes de fonctionnement 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.

Problématique retenue

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.

Objectifs du TIPE

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

Références bibliographiques (ETAPE 1)

[1] Wikipédia : Advanced Encryption Standard :
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 :
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/*

DOT

[1] *Février 2021 à Juin 2021 - Etude de l'algorithme AES et des structures mathématiques associées. Développement en parallèle d'un prototype en OCaml.*
[2] *Septembre 2021 à Janvier 2022 - Etude du format PNG et de la structure brute d'une image.*

Application de l'algorithme à une image en la lisant directement et en décodant le fichier.

[3] *Janvier 2022 à Mars 2022 - Développement d'une application pour iPhone, afin de récupérer des données de santé depuis l'Apple Watch, que nous avons chiffré.*

[4]