14454 LESTIENNE Thibault

Application des transducteurs finis à la cryptographie

Après le visionnage du film Enigma, je me suis intéressé à la cryptographie et à son histoire. J'ai découvert son importance accrue par l'évolution des échanges numériques. Cela m'a donné l'envie d'en faire le thème de mon TIPE.

J'ai décidé de m'intéresser à la cryptographie qui cherche à transformer un message afin de le transmettre sans qu'il puisse être compris par une autre personne que son destinataire. Cela s'inscrit donc dans le thème transition, transformation, conversion.

Positionnement thématique (ÉTAPE 1) :

- *INFORMATIQUE (Informatique Théorique)*
- *INFORMATIQUE (Informatique pratique)*

Mots-clés (ÉTAPE 1) :

Mots-clés (en français)	**Mots-clés (en anglais)**
Automates finis	*finite-state automatons*
Transducteurs finis	*finite-state transducers*
Cybersécurité	*Cybersecurity*
Cryptographie	*Cryptography*
Machine de Mealy	*Mealy machine*

Bibliographie commentée

L'évolution de la cryptographie et des outils associés a permis de renforcer considérablement la sécurité des échanges privés à travers l'histoire, particulièrement dans les domaines politiques et militaires. Elle continue aujourd'hui d'être essentielle dans un monde numérique de plus en plus interconnecté, en protégeant échanges privés et paiements en ligne.[1/2]

Le chiffre de César dès le premier siècle avant notre ère fut l'un des premiers systèmes de chiffrement utilisés. Il consistait à décaler chaque lettre d'un message d'un certain nombre de positions dans l'alphabet. Cette méthode était simple et rapide à mettre en place mais facile à décoder pour un attaquant s'emparant du message, ce qui ne le rendait que peu utile en pratique. [2/3]

Le chiffre de Vigenère a été découvert en 1500. La principale différence entre le chiffre de César et le chiffre de Vigenère réside dans le fait que, dans le chiffre de César, le décalage appliqué à chaque lettre est constant et identique pour tout le message, tandis que dans le chiffre de Vigenère, le décalage varie en fonction de la clé, ce qui rend le chiffrement plus complexe et difficile à déchiffrer sans connaître la clé. Il sera considéré comme l'un des meilleurs algorithmes de chiffres pendant plus de trois siècles, jusqu'à sa cryptanalyse en 1854. [3]

En 1883, Auguste Kerckhoffs énumère ses six principes parmi lesquels on retient encore aujourd' hui les deux premiers : "Le système doit être matériellement, sinon mathématiquement indéchiffrable" et "Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi". [4]

La cryptographie prendra une place encore plus prépondérante durant la Seconde Guerre mondiale, où Alan Turing décryptera avec succès les messages encodés par la machine allemande Enigma donnant un avantage significatif aux alliés. [3]

En 1977, le chiffrement RSA est le tout premier chiffrement asymétrique à être découvert. Il ouvre un nouveau champ de possibilités dans le domaine de la cryptographie en permettant à deux individus de communiquer de manière sécurisée sans s'accorder au préalable sur une clé commune. [3/5]

Les transducteurs sont des objets informatiques qui dans la théorie des langages formels permettent de transformer un mot en un autre mot via un processus déterministe. Ils ont aujourd'hui trouvé de nombreuses applications dans les domaines de la linguistique ou de la correction orthographique. [6]

Problématique retenue

Les transducteurs finis peuvent-ils contribuer à sécuriser des échanges privés ?

Objectifs du TIPE du candidat

• Implémenter un système cryptographique à partir de transducteur

• Rechercher des vulnérabilités

• Tester la résistance face à des outils de déchiffrement automatique

• Comparer à d'autres méthodes de chiffrement

Références bibliographiques (ÉTAPE 1)

[1] STÉPHANIE DELAUNE : Protection des données: le chiffrement ne suffit pas *: https://lejournal.cnrs.fr/billets/protection-des-donnees-le-chiffrement-ne-suffit-pas*

[2] JACQUES STERN, LOUIS GRANBOULAN, PHONG NGUYEN, DAVID POINTCHEVAL : Conception et preuves d'algorithmes cryptographiques *: https://www.di.ens.fr/~granboul/enseignement/crypto/CoursCrypto.pdf*

[3] JOSH SCHNEIDER : Historique de la cryptographie : Un aperçu des méthodes de transmission de messages secrets au fil des siècles. *: https://www.ibm.com/fr-fr/think/topics/cryptography-history*

[4] WIKIPEDIA : Principe de Kerckhoffs *: https://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs*

[5] R.L. RIVEST, A. SHAMIR, AND L. ADLEMAN : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems *: https://people.csail.mit.edu/rivest/Rsapaper.pdf*

[6] TÉLÉCOM PARIS : Le modèle « transducteur fini » *: https://perso.telecom-paristech.fr/jsaka/ENSG/MITRO204/Files/Lectures/TRNS-L1-161206.pdf*