Rapport Scientifique et Technique
L3 SPI – Module Expression Scientifique et Technique – 2014-2015

La Cryptographie

SAID AHMED Mahamoud & DIDIER Mathias

10 février 2015

Résume

Notre sujet porte sur un thème bien connu par les informaticiens et les historiens : il s'agit de l'univers de la Cryptographie.
L'étude de ce sujet s'étend sur trois grandes parties relatant du cryptage sous trois angles : technique et applicatif de la cryptographie, les menaces et les solutions.
La notion de cryptographie remonte à l'Antiquité durant laquelle les Grecs utilisaient des outils primaires pour envoyer des messages codés. La nécessité de vouloir crypter un message s'est manifestée par la volonté d'empêcher une tierce personne autre que le destinataire à décrypter le message. Plus tard, les outils de cryptographie se sont perfectionnés ainsi que les méthodes de chiffrement dans le but de transmettre plus rapidement et plus efficacement un message. Chaque guerre apporta son lot de perfectionnement au service de la stratégie militaire, car un message crypté attire une plus grande attention qu'un message en clair. Tôt ou tard, suivant la technologie et le génie d'une personne, il sera décrypté.
De nos jours, la cryptographie est utilisé dans de nombreux domaines : militaire, informatique, financier, sécurité... et permet de sécuriser les flux d'informations. Les exemples de programmes écrits par des étudiants montrent à quel point l'avenir de la cryptographie est prometteur.

Table des matières

1- Introduction

La cryptologie est née avec l'apparition de l'écriture et fut justifiée par le besoin de protéger tout message écrit afin d'éviter que l'ennemi ne puisse, en se l'appropriant, exploiter les renseignements qu'il contenait. Littéralement « science du secret », elle a longtemps été associée à de mystérieux enjeux d'espionnage militaire et diplomatique bien éloignés des préoccupations scientifiques. La cryptographie est quant à elle, l'ensemble des techniques constituant la cryptologie.
Ses premières formes furent le plus souvent basiques, mais avec l'évolution des peuples des technologies et des « casseurs de codes », son développement est en constante recherche de progression. Comment la cryptologie émergea ? Où en est elle de nos jours ? Quel avenir a-t-elle ?
A l'époque de Jules César, des méthodes rudimentaires permettaient de rendre ses ordres « incompréhensibles » à ses adversaires. Néanmoins, l'absence de rigueur des concepteurs de ces systèmes mena à des failles qui permettaient à leurs adversaires de comprendre les messages malgré tout.
De nos jours l'information sous toutes ses formes : voix, images, œuvres musicales, textes et autres, circule au format numérique à travers le monde en une fraction de seconde. Que ce soit par le téléphone, le câble, les fibres optiques ou par satellite, cette information est chaque jour échangée d'un point à un autre et se trouve susceptible d'être lue, copiée, supprimée, altérée ou falsifiée. La cryptologie répond aujourd'hui aux besoins du marché et constitue un domaine scientifique en pleine activité. Elle intervient dans de multiples applications et représente l'élément essentiel de la sécurisation du commerce électronique et du réseau Internet.
La transmission d'un message codé qui se veut sûr doit satisfaire les trois conditions suivantes :

- Confidentialité : la technique de cryptage se doit de garantir le secret de l'information, aucun tiers ne doit pouvoir lire le message.
- Intégrité : le cryptosystème ne doit engendrer aucune absence de modification de l'information, et le message ne doit pas pouvoir être modifié durant son « transport ».
- Authenticité : le codage du message doit garantir l'origine de l'information, le message doit annoncer son émetteur sans le trahir.

Nous allons dans un premier temps vous présenter quelques différents types de cryptages, à savoir les méthodes cryptographiques permettent le chiffrement par substitution, par transposition et par clé. Puis, nous allons tenter, à travers la deuxième partie, parler des certains menaces ; Enfin, nous vous présenterons quelques solutions envisageables.

1.1- Cadre et but du document

2- Partie 1 : Le chiffrement

Le chiffrement garantit la confidentialité. Autrement dit, il protège l'information contre toute divulgation non autorisée ou toute visualisation par le brouillage mathématique du texte original.

Le chiffrement par substitution :

Les chiffrements par substitution fonctionnent en ajoutant ou supprimant chaque caractère par la clé. Ainsi pour une clé de 3, la valeur de « aa » devient « dd ».
La clé peut aussi être une chaîne de caractères, ainsi la valeur de la clé pour un caractère sera le caractère « courant » de la clé, et pour le caractère a chiffrer suivant, la valeur de la clé est le caractère suivant dans la clé, et si la clé est fini, elle reprend la valeur du début.

Le chiffrement par transposition :

Les chiffrements par transpositions fonctionnent de tel sorte que le message soit coupé en blocs de même tailles, et des anagrammes sont crées pour chacun des blocs; il s'agit d'inverser l'ordre des lettres dans un même bloc.
Des caractères (dits de bourrages), peuvent être ajoutés à chacun des blocs pour complexifier le procéder de cryptanalyse.
La clé est la permutation d'elle même (voir tableau de permutation).
Le nombre de permutation possible est la factorielle de la taille des blocs : ainsi, plus les blocs sont longs, plus il y aura de possibilités de permutations possibles (ex : taille = 3 => 6 positions possibles ; taille= 20 => 432 902 008 176 640 000 positions possibles (20!))

Le chiffrement par clé :

Les systèmes à conventions restreintes présentent une faille principale :

- ils nécessitent que l'algorithme soit secret.

C'est pourquoi la création de systèmes à clé sont maintenant utilisés, ils permettent d'avoir un algorithme connu de tous.

3- Partie 2: Les menaces

Le but de la cryptographie étant de protéger le caractère confidentiel d'une information donnée.
Il existe plusieurs méthodes liées à la cryptanalyse pour tenter de déchiffrer un message.

4- Partie 3 : Les solutions

Les solutions pour chiffrer des données sont assez variés:

- pour un chiffrent symétrique :
    1. le Data Encryption Standart(DES (1975))
    2. l'international Data encryption algorythm(IDEA, 1990)
    3. Advanced Encryption Standart (le plus recent (2000), utilisé par la NASA)

- pour un chiffrement asymétrique :
    1. RSA(du nom de ses inventeurs) 1977
    2. Digital Signature Standart (DSS 1993-6)
    3. Digital Signature Algorythme (DSA 1994)