45927 PEA Romain

La Cryptanalyse des méthodes de substitutions alphabétiques

La cryptographie permet la résolution des problèmes liés à la nécessité de dissimuler des informations , linguistiques au début, puis numériques avec le développement des technologies de la communication.
J'étudierai différentes méthodes permettant de faciliter les interactions entre les divers protagonistes,de celui qui émet le message codé à celui qui le reçoit, au moyen d'algorithmes de chiffrement et de déchiffrement.

Positionnement thématique (phase 2)

INFORMATIQUE (Informatique pratique), MATHEMATIQUES (Mathématiques Appliquées), INFORMATIQUE (Informatique Théorique).

Positionnement thématique (phase 3)

INFORMATIQUE (Informatique pratique), INFORMATIQUE (Informatique Théorique), INFORMATIQUE (Technologies informatiques).

Mots-clés (phase 2)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Algorithme	*Algorithm*
Cryptanalyse	*Cryptanalysis*
Cryptographie	*Cryptography*
Chiffrement	*Encryption*
Arithmétique	*Arithmetic*

Bibliographie commentée

La cryptographie est la science du développement de méthodes de chiffrement d'un message dit « en clair » vers un message dit « codé » à l'aide d'une clef de chiffrement pour ce qui est des méthodes de substitutions alphabétiques. Cette technique doit aussi permettre le déchiffrement du message « codé » vers le message initial « en clair ».

La cryptanalyse est l'étude mathématique et informatique de ces méthodes dans le but de « casser » cette méthode , c'est à dire de trouver un moyen , souvent un algorithme , de trouver la clef de chiffrement quel que soit le texte chiffré , pour ainsi le déchiffrer à coup sûr [1].

De nombreuses utilisations des méthodes cryptographiques , bien souvent militaires , sont à dénombrer . On peut ainsi distinguer :
_ Les méthodes de César , datant de l'Antiquité romaine , permettant aux armées de Jules César de communiquer sans être compris . Cette méthode est considérée généralement comme la méthode

de substitution alphabétique la plus simple , consistant à décaler la lettre utiliser d'un nombre constant de rang dans l'alphabet latin, et sa cryptanalyse reste simple.
_ La méthode de Vigenère , un peu plus compliquée , avec une méthode dérivée de César , a permis de mettre à l'épreuve les premiers vrais cryptanalystes au 17e siècle , mais , malgré la difficulté un peu plus élevée que pour une simple méthode de César , la cryptanalyse reste abordable [2] grâce aux redondances dans le chiffrement.
_ La méthode Enigma , utilisée par les nazis lors de la seconde guerre mondiale , a requis le travail acharné des plus grands mathématiciens de l'époque , y compris Alan Turing , père de l'Informatique à bien des égards , à cause de la rotation des rotors composant la machine à écrire « chiffrante » Enigma , c'est à dire que la clef changeait à chaque lettre et la cryptanalyse , sans ordinateurs à l'époque , est devenue compliquée [3].

Toutes ces méthodes nous montrent des failles , puisqu'elles ont été cassées , et leurs études , ainsi qu'une étude arithmétique [4] des rouages mathématiques se dissimulant derrière chaque méthode , permettra l'imagination d'un nouveau procédé dans la substitution alphabétique , auquel il faudra éviter les lacunes des méthodes cryptanalysées ci dessus.

La mise en œuvre d'une telle méthode sera aidée algorithmiquement par une programmation python permettant la sollicitation de la puissance informatique contemporaine , ce que les créateurs des méthodes étudiées ne possédaient pas.

Il faudra bien sûr garder à l'esprit que les méthodes de substitution alphabétiques utiles , c'est à dire cryptographiques , qui peuvent se déchiffrer après chiffrement , seront , de toutes façons , moins performantes que les méthodes cryptographiques plus moderne , comme le hachage elliptique [5] .

Problématique retenue

Comment , à partir de cryptanalyses de méthodes de chiffrement plus ou moins avancées , trouver un chiffrement plus sûr par déduction des failles des précédents ?

Objectifs du TIPE

-- **Analyser** les méthodes les plus récurrentes du cryptanalyste lorqu'il tente une attaque sur une méthode de substitutions alphabétiques.
-- **Synthétiser** , à l'aide des méthodes cryptanalytiques , les erreurs à ne pas commettre lors de l'imagination et de la mise en oeuvre de ce genre de méthodes.
-- **Proposer** alors une approche cryptographique permettant d'éviter ces "écueils" , le but final étant d'essayer de développer un algorithme fonctionnel sur Python permettant de chiffrer un message avec la méthode de substitution proposée.

Abstract

Cryptography is being increasingly used with the growth of the internet. I took a special interest in

alphabetical substitution methods. These kinds of methods are based on the replacement of characters by others. I started studying some classical methods to understand what is important to create a good one. Then, I created mine, and finally, I tried to improve my methods through the study of the best-known methods I was taught.

Références bibliographiques (phase 2)

[1] ? : "Cryptanalyse" ; Wikipédia : *https://fr.wikipedia.org/wiki/Cryptanalyse#Cryptanalyse_%CF%87%C2%B2*

[2] Luca De Feo : "Cryptanalyse de Vigenère" : *http://defeo.lu/in420/Cryptanalyse%20de%20Vigen%C3%A8re%20-%20DM*

[3] Fred Bayart : "Principe de fonctionnement de la machine Enigma" : *http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/enigmafonc*

[4] Gilles Zémor : "Cours de Cryptographie" : *une grande partie de l'ouvrage m'a servi toute l'année ; Editions Cassini ; 2001*

[5] Mehdi Tibouchi : Thèse de Doctorat ; "Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA" : *2011 ; Université Paris-Diderot ; consultée en novembre 2017 , a servi principalement à l'approfondissement de ma culture cryptographique , en vu d'autres méthodes de chiffrement*

DOT

[1] *Début, durant l'été dernier, de la réflexion concernant les bases des méthodes cryptographiqes qui seront présentées, premières mises en œuvre algorithmiques des méthodes, premières approches factuelles des problèmes de ces méthodes*

[2] *Etudes de méthodes connues, dans le but de comprendre la cause des problèmes dans les méthodes proposées, lors du premier trimestre de l'année en cours*

[3] *Synthèse des écueils à éviter*

[4] *Amélioration significative de la première méthode , au moyen d'une variation en temps réel de la clef de chiffrement*

[5] *Abandon de la deuxième méthode en avril , regroupant une grande partie des problèmes qui avaient été listés comme étant «à éviter»*

[6] *Reprise de la deuxième méthode fin mai, car jugée exemple important de ce qui est possible d'imaginer, mais présentant des carences la rendant non viable*

[7] *Réussite complète dans le même temps de ce qui avait été prévu de mettre en œuvre concernant la première méthode*

[8] *Problème concernant la mise en œuvre finale de la seconde méthode , concernant la taille des éléments caractéristiques de cette méthode, trop volumineux pour que des ordinateurs classiques puissent se servir efficacement des algorithmes associées à la méthode*