Cahier Des Charges

Alabi Steve - Benyamna Younes - Capdenat Nicolas-
Chouipe Thibaut - El Harti Zakaria - Lienhardt Florian

Chef de projet : Benyamna Younes

Sous la direction de Mme Kloul

Outil automatique de décryptage

22 mars 2017

1 Preambule

La steganographie, qui est "l'ancêtre" de la cryptographie. Elle se définit comme l'art de cacher un message dans un autre message. Cet "art" est appelé art de la dissimulation. Par exemple ,la lettre de Georges Sand à Alfred Musset(la subtilité réside ici dans le fait qu'il faut lire une ligne sur deux de la lettre pour découvrir le vrai message). Cependant, cet art présente une importante contre-mesure. En effet, si le message dissimulé est decouvert, le contenu secret esr revelé.

Ainsi, un autre "art" s'impose : il est appelé art du secret et c'est justement la cryptographie. signifiant lui "écrire". En effet, comme le dit Ronald Rivest, grand cryptologue américain et l'un des 3 inventeurs de l'algo de crypto à clé publique RSA, la crypto est la pratique et études des techniques pour assurer des communications sûres en présence d'adversaires. Trois critères doivent etre respectés : -confidentialité : personne ne doit lire le message et on doit protéger le contenu. -authenticité : personne ne doit contrefaire l'origine du message et on doit s'assurer de la provenance de celui-ci. -intégrité : personne ne doit modifier le message et on doit s'assurer de la non-modification de celui-ci.

La cryptographie, ainsi que la cryptanalyse(tout simplement l'art de rendre clair un texte crypté sans avoir connaissance de la clef utilisée) constituent la cryptologie. C'est un art ancien qui a commencé au 16eme siècle avant J-C et c'est egalement une science nouvelle car elle est encore utilisée de nos jours dans plusieurs domaines tels que les banques(cartes), le web(navigateurs)..etc
Au 21éme siecle, une nouvelle forme de cryptographie liée a l'ère de l'informatique est apparue.

Voici ci-dessous un tableau récapitulatif des différents chiffrements les plus connus :

Symétrique		**Asymétrique**
Mono	**Poly**	**l'ere informatique**
Decalage	Hill	SSL
Affine	Enigma	DES
Chaine	Porta	RSA
Permutation	ADFGVX	Fn de hachage
Substitution	Vigenere	

2 Explications du chiffre de Vigenère et du chiffrement par substitution

Nous allons lors de nôtre projet nous interesser aux deux chiffrements suivants.
Pré-condition : Avoir un texte suffisament grand.

2.1 Analyse Fréquentielle

L'analyse frequentielle compte le nombre de lettres du texte pour détérminer sa taille et compte le nombres d'occurences de chaques lettres. Elle calcule ensuite la probabilité d'apparition de chaque lettre. Enfin elle compte le nombre des digrammes et trigrammes les plus utilisés.

2.2 Vigenère

2.2.1 Chiffrement

Soit pour chaque lettre de l'alphabet son indice lui correspondant(a=0,b=1..z=25).
Le chiffrement de Vigenère consiste à additionner les valeurs de chaque lettre du texte clair avec celles d'un mot-clé qui va se repeter.
Au résultat on appliquera un modulo 26 afin d'être sûre de retomber sur une valeur numérique(entre 0 et 25), et donc correspondant a une lettre de l'alphabet.

2.2.2 Dechiffrement

Le dechiffrement de Vigenère est basé sur une méthode d'attaque statistique.
On commence par effectuer le test de Kasiski : on cherche des paires de chaines de caractères identiques de longueur > 2 dans le texte chiffré et on note la distance entre les premiers caractères D1.
Si l'on obtient plusieurs distances D1, D2, .. Di, alors on peut conjecturer que le PGCD des Di est la taille m de la clef.
Ensuite, on va chercher les caractères qui composent notre mot-clef. Nous allons utiliser l'indice de coincidence. Dans une langue usuelle, les lettres n'apparaissent pas toutes avec la même fréquence. C'est pourquoi l'indice de coincidence d'un texte en francais (=If) est très supérieur à l'indice de coïncidence d'un texte aléatoire (=Ia) où les lettres ont une fréquence d'apparition identiques. Ainsi une analyse statistique sur de nombreux textes a donné If=0,074, tandis qu'un petit calcul donne Ia=0,038 (=1/26) Pour chaque caractère du mot clé, on va faire le Mg correspondant à une lettre sur m sur le texte a décrypter. ($0 <$ g <25)

$M_g = \sum_{i=0}^{25} \frac{P_i F_{i+g}}{n'}$
n' = n/m
Pi = probabilité d'apparition d'une lettre dans un texte en francais
Fi = Frequence d'apparition d'une lettre dans un texte chiffré

On va donc obtenir un tableau de m lignes contenant chacunes 26 valeurs et remarquer que une seule valeur par colonne se rapproche de 0,074(=If).
On va donc pouvoir en deduire les valeurs des caractères du mot-clé. Pour finir, on va soustraire le mot-clef (on le repete autant de fois que nécessaire) au texte chiffré afin d'obtenir le texte clair.

2.3 Substitution

2.3.1 Chiffrement

La méthode de cryptage par substitution monoalphabétique consiste a remplacer dans un message en clair chaque lettre de l'alphabet de ce message par une lettre d'un alphabet donné. Deux lettres distinctes de l'alphabet du message en clair doivent être chiffrés par deux lettres distinctes de l'alphabet donné afin d'éviter toute ambiguïté lors du déchiffrement.

2.3.2 Dechiffrement

Le décryptage de la substitution monoalphabétique est basé sur une méthode d'attaque statistique utilisant l'analyse fréquentielle. Il faut donc que le texte crypté soit assez long pour une analyse statistique. On compare ensuite les résultats de l'analyse fréquentielle aux nombres d'occurrences de chaque lettre de l'alphabet en clair. Il faut donc connaître la langue correspondant au texte a décrypter. On conjecture alors les correspondances entre les lettres de l'alphabet en clair et de l'alphabet crypté. On complète ensuite cette correspondance grace a une analyse des digrammes et des trigrammes les plus utilisés dans la langue de l'alphabet en clair. On possède alors un message partiellement décrypté du message en clair.

3 Numerotation des exigences

4 Fondement du projet

4.1 Problème de l'utilisation ou contexte du projet

Dans le cadre de notre L3, nous devons concevoir un programme d'aide au decryptage. Grace a notre programme le client(ici notre enseignante Mme Kloul) va évaluer nôtre travail.

4.2 Objectif de la section

L'objectif de ce module est de nous apprendre a travailler efficacement en equipe afin de fournir un travail commun.

4.3 Objectif du projet

Le but du projet est de réaliser un logiciel automatique d'aide au décryptage, capable de retrouver une grande partie du texte d'origine à partir d'un texte chiffré. Il devra aussi être capable de déchiffrer le chiffrement de Vigenère et le chiffrement par substitution.

5 Contraintes sur le projet

5.1 Contraintes sur la conception de la solution

-Le produit doit permettre à l'utilisateur de décrypter une partie d'un message crypté. -Le produit doit crypter ou décrypter un chiffrement de Vigenère et un chiffrement par substitution. -Toutes les deadlines concernant l'application et son cahier des charges doivent être respectées.

5.2 De combien de temps les développeurs disposent-ils pour le projet ?

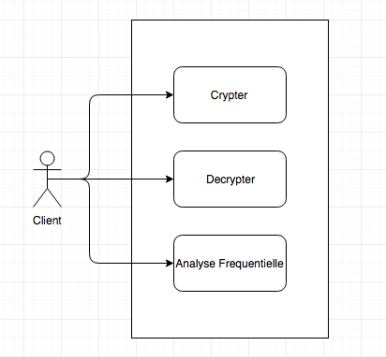
La deadline pour les développeurs est le Vendredi 12 Juin 2017.

5.3 Conventions de dénomination

k est la clé m est la taille de la clé n est la taille du message chiffré

6 EXIGENCES FONCTIONNELLES

6.1 Portée du produit : cas d'utilisation



Dans cette application il n'y a qu'un seul type d'utilisateur qui est le client et qui peut crypter et decrypter avec deux méthodes différentes à disposition. Il pourra également faire une analyse fréquentielle sur le texte donné.

7 EXIGENCES NON FONCTIONNELLES

7.1 Ergonomie et convivialité du produit

L'interface permettra de rentrer facilement le texte à décrypter, par copier-coller par exemple. De plus, l'interface permettra de choisir la langue (anglais, français) grâce à un simple menu. Enfin, l'interface permettra aussi d'afficher facilement le resultat obtenu. Le programme sera évalué par la responsable du module Projet de la L3 donc il doit apparaître simple et effiace (pas de superflu). Le programme ne doit pas être trop gros en terme de resolution, on doit pouvoir l'afficher sur tous les types d'écrans d'ordinateurs.

7.2 Facilité d'utilisation

Le programme sera simple à utiliser même pour un enfant. Le programme pourra etre utilisé par des personnes sans qu'elles y soient formées.

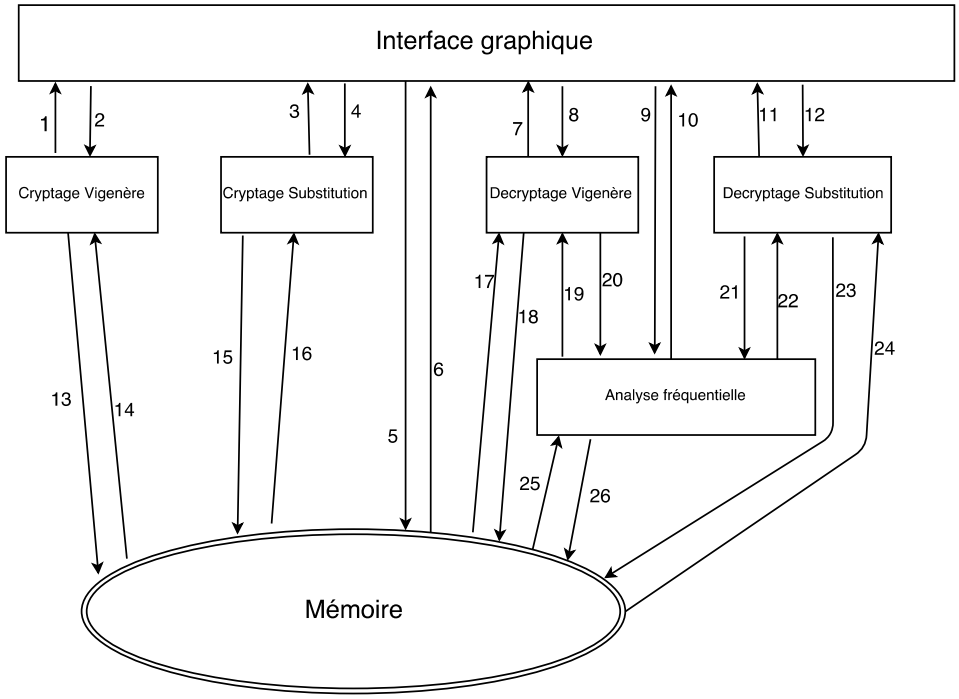
8 AUTRES ASPECTS DU PROJET

8.1 COTS : progiciels et composants commerciaux

Il existe sur le marché pas mal de produits pouvant être des solutions potentielles/de remplacement :
-www.dcode.fr : site proposant de decrypter votre texte.
-Decrypto : disponible sur le Google Play Store et gratuit.
-Axcrypt : logiciel gratuit.

8.2 Tâches à faire pour livrer le système

Phase I : Identification du projet : La demande du client est clarifiée, les objectifs précisés et dans sa globalité le projet est identifié.
Phase II : Definition du projet : Son contenu est defini de maniere tres precise et la planification des echeances et de la repartition du travail est etablie.
Phase III : Realisation : On realise le projet en adequation avec les exigences du clients et selon le plan de travail defini au prealable.
Phase IV : Finalisation : Le produit est evalué puis remis au client.



1) Un ensemble de données contenant le texte crypté
2) Un nom de fichier
3) Un ensemble de données contenant le texte crypté
4) Un nom de fichier
5) Un nom de fichier
6) Fichier texte : clair, crypter, décrypter ou analyse fréquentielle
7) Un ensemble de données contenant le texte en clair
8) Un nom de fichier
9) Un ensemble de données contenant l'analyse fréquentielle
10) Un nom de fichier
11) Un ensemble de données contenant le texte décrypté ou le texte clair
12) Un nom de fichier
13) Un nom de fichier
14) Fichier texte clair
15) Un nom de fichier
16) Fichier texte clair
17) Un fichier texte crypté
18) Un nom de fichier
19) Un ensemble de données contenant l'analyse fréquentielle
20) Un nom de fichier
21) Un nom de fichier
22) Un ensemble de données contenant l'analyse fréquentielle
23) Un nom de fichier
24) Un fichier texte crypté
25) Un fichier texte en crypté ou en clair
26) Un ensemble de données contenant l'analyse fréquentielle

8.3 Organigramme

Interface graphique :
- bouton cryptage
- bouton decryptage
- bouton substitution
- bouton Vigenère
- affichage de texte(complet et partiel)
- affichage pour la clé de substitution
- bouton Francais(decryptage)
- bouton Anglais(decryptage)
- affichage pour l'analyse fréquentielle
- charger un fichier texte
- sauvegarder un fichier texte
- créer un nouveau fichier texte(resultats)
- Demander clef de Vigenère

Decryptage Vigenère :
-decrypter le message

Cryptage Substitution :
-créer une clé aleatoirement
-crypter le message

Cryptage Vigenère :
-crypter le message

Decryptage Substitution :
-decrypter le message

Analyse fréquentielle :
-analyse frequentielle sur texte donné

8.4 Estimation des coûts du projet

Module	Cout (ligne)	Personne(s) en charge
Décryptage Vigenere	200	Chouipe & Alabi
Décryptage Substitution	150	Lienhardt & Alabi
Cryptage Vigenere	50	El Harti
Cryptage Substitution	50	El Harti
Analyse Fréquentiel	50	El Harti
Interface Graphique	1000	Benyamna & Capdenat
Total	1500	

8.5 Manuel utilisateur et formations à envisager

L'utilisateur aura accés à un menu lui permettant de choisir de crypter ou décrypter un texte, puis la méthode qu'il veut utiliser pour ce faire (vigenere ou substitution), il ne lui restera plus qu'a importer son texte.

8.6 Salle d'attente : idées pour les futures versions

Bien que le programme ait été demandé que pour la langue francaise et anglaise, il sera sans doute possible d'ajouter d'autres langues dans des versions futurs. Il pourra être également possible d'ajouter une option permettant à l'utilisateur d'entrer un type de texte (poème, roman, ordre militaire,...) pouvant aider au décryptage. Ou même encore conserver un historique des "dechiffrements" ou aussi permettre a l'application de savoir directement si l'on va crypter ou decrypter un texte.

9 Choix du language

Après l'analyse des besoins et après avoir constaté que la programmation orienté-objet n'etait pas nécessaire, nous avons donc choisi d'utiliser le langage C. C'est en effet un langage procédurale et performant. De plus, toute l'equipe le maitrise, entrainant ainsi une diminution des coûts liée a un eventuel temps de formation. La bibliothèque graphique que nous avons décidée d'utiliser avec ce langage est GTK+ parce qu'elle permet d'implémenter des boutons, des zones de texte et du traitement de fichier. Elle nous semblait donc la plus adaptée au developement de notre application.

10 Conclusion

Afin de répondre aux attentes/besoins du client, nous proposons l'application Dcrypt. Elle permet de décrypter facilement un texte chiffré avec le chiffrement de Vigenère ou de Substitution. Cette application permettra également au client de réaliser une analyse fréquentielle sur un texte chiffré. D'autre part elle permettra de chiffrer un texte clair avec le chiffrement de Vigenère ou de Substitution.
Ce cahier des charges a été réalisé par une équipe de 6 étudiants de licence en informatique. Etant le premier cahier des charges pour chacun de nous, cela nous a permis de nous projeter dans une situation plus professionnelle et d'avoir une organisation de travail différente suivant un modèle bien précis (ici, Volère).

11 Sources

Liens(Sites) :
fr.wikipedia.org/wiki/cryptographie
fr.wikipedia.org/wiki/cryptanalyse
fr.wikipedia.org/cryptologie
e-campus.uvsq.fr/cours/chribour/cours-chribour-20140220133009
www.thawte.fr/assets/documents/guides/history-cryptography.pdf
mantis.free.fr/articles/analyse.htm
https ://fr.slideshare.net/mobile/antoningaunaud/les-4-phases-du-management-de-projet-2889991
www.volere.co.uk/template-fr
www.bibmath.net/crypto
Livres :
Cryptographie : Théorie et pratique, de Douglas Stinson
Cryptologie et codage : comprendre les codes secrets, de Pierre Vigoureux