Cahier Des Charges

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

21 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 :

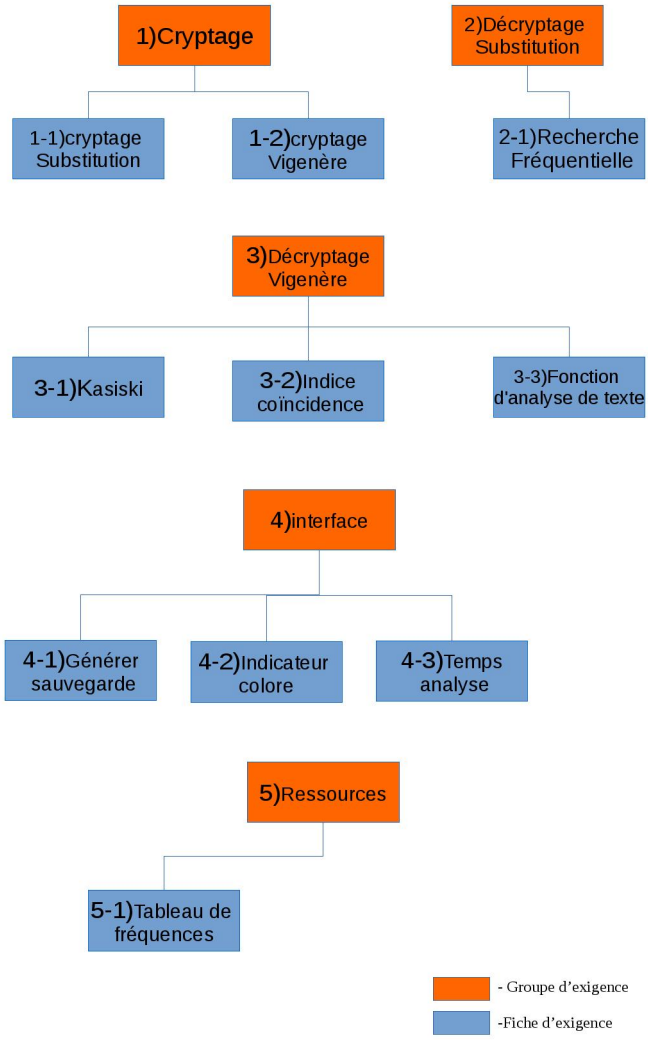
Symétrique		**Asymétrique**
Mono	**Poly**	**l'ere informatique**
Decalage	Hill	SSL
Affine	Enigma	DES
Chaine	Porta	RSA
Permutation	ADFGVX	Fn de hachage
Substitution	Vigenere	

Nous allons lors de nôtre projet nous interesser aux deux suivants :
Soit pour chaque lettre de l'alphabet son indice lui correspondant(a=0,b=1..z=25)
-Vigenère :
Le chiffrement de Vigenère consiste à faire une addition du texte en clair avec la clé(faire modulo 26).
Le dechiffrement lui se fait par soustraction du texte avec la clé ou à l'aide du test de Kasiski et de l'indice de coincidence si on ne connait pas la clé.
-Substitution :
Son chiffrement génère un nouvel alphabet : une lettre correspondra à une seule nouvelle lettre. Puis on utilise ce nouvel alphabet pour remplacer les lettres du texte clair. Le dechiffrement(avec connaissance de l'alphabet) consiste à effectuer l'operation précedente dans le sens inverse(chiffrement a->t,dechiffrement t->a). Sinon on effectue une analyse frequentielle afin de retrouver l'alphabet.

2 Fiches d'exigence

Vous trouverez les fiches d'exigences en annexe.

3 Numerotation des exigences



4 Fondement du projet

4.1 But du projet

4.1.1 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 le professeur) va évaluer nôtre travail.

4.1.2 Objectif de la section

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

4.1.3 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.

4.2 Personnes et organismes impliqués dans les enjeux du projet

4.2.1 Maitre d'ouvrage

Ce projet fait partie du module projet de la 3eme année d'informatique dirigé par Mme Kloul qui travaille au sein de l'UVSQ.

5 Contraintes sur le projet

5.1 Contraintes imposées non negociables

5.1.1 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.

5.1.2 Environnement de fonctionnement du système actuel

Le produit sera développé sous forme d'application. Le programme s'appuiera essentiellement sur des recherches fréquentielles pour décrypter un chiffrement par substitution et utiliser le test de Kasiski et les indices de coincidences pour déchiffrer par Vigenere.

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

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

5.2 Glossaire et conventions de dénomination

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

5.3 Faits et hypothèses utiles

5.3.1 Facteurs influençant le produit, mais qui ne sont pas des contraintes imposées sur les exigences

Mettre en place une interface facile d'utilisation sur l'application de manière a ce que même un enfant puisse lancer le décryptage.

6 EXIGENCES FONCTIONNELLES

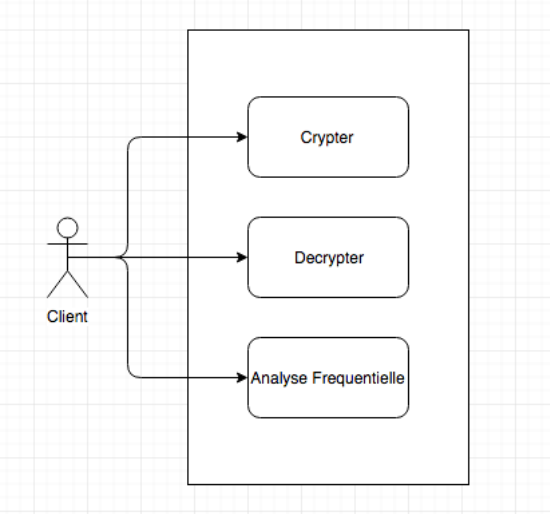
6.1 Portée du travail

6.1.1 Contenu du travail

Il est nécessaire de connaitre le chiffrement et le déchiffrement (avec et sans clé) de Vigenère et de substitution.

6.2 Portée du produit : cas d'utilisation

6.2.1 Le diagramme de cas d'utilisation



6.2.2 Description de ce diagramme

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.

6.3 Exigences fonctionnelles et exigences sur les données

6.3.1 Exigences fonctionnelles

Fiches d'exigences numero : 2.1 / 3.1 / 3.2 / 3.3 / 5.1

7 EXIGENCES NON FONCTIONNELLES

7.1 Ergonomie et convivialité du produit

7.1.1 L'interface

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.

7.1.2 Le style du produit

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 et facteurs humains

7.2.1 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.

7.2.2 Personnalisation et internationalisation

Le programme sera trop simple pour etre personnalisable et il sera en anglais(simple a la compréhension).

7.2.3 Facilité d'apprentissage

Le developpement d'un site web présentant le produit ainsi que toutes ses caractéristiques. Ce site web pourra également disposer d'un forum permettant aux internautes de proposer certaines améliorations à faire sur l'application et également critiquer certaines fonctionnalités de l'application. Il sera possible au grand public d'utiliser le programme sans formation.

7.2.4 Facilité de compréhension et politesse

Le produit devra utiliser des symboles et des mots naturellement compréhensibles par les utilisateurs potentiels. Le produit doit cacher les détails de sa construction à l'utilisateur.

7.3 Fonctionnement du produit

7.3.1 Rapidité d'exécution et temps de latence

La réponse sera assez rapide pour éviter d'interrompre le flux de pensée de l'utilisateur.

7.3.2 Précision et exactitude

C'est un programme d'aide au décryptage donc il ne donnera jamais un texte complet en sortie mais un "texte à trou" rempli au mieux avec le résultat du décryptage.

7.4 Adéquation du produit avec son environnement

7.4.1 Environnement technologique prévu

Le programme pourra fonctionner sur Windows, Linux et Mac.

7.4.2 Approche « produit » prêt à être commercialisé

Le programme sera distribué sous forme d'archive correspondant au système d'exploitation du client.

7.5 Maintenance, support, portabilité, installation du produit

7.5.1 Maintenance du produit

Le système doit pouvoir être maintenu par des développeurs qui ne sont pas les développeurs d'origine. Mettre en place une gestion des erreurs ou bugs (par exemple a l'aide de tests unitaire, d'indicateurs comme des variables..etc).

7.5.2 Conditions spéciales concernant la maintenance du produit

Site internet avec des informations sur l'application. Permettre également un dialogue avec d'autres utilisateurs de la même application. Demandes d'aide aux développeurs chargés de la maintenance de l'application.

7.5.3 Exigences de portabilité

L'application peut fonctionner sur plusieurs environnements car "un makefile est fourni et permet a l'utilisateur de build en fonction de son environnement"(comme linux, windows ou autre).

7.5.4 Installation du système

L'application doit pouvoir être installée très facilement sur n'importe quel environnement. Le site internet doit permettre de répondre à certaines interrogations.

7.6 Sécurité

7.6.1 Intégrité

Definition d'un niveau d'importance de "l'exactitude" nécessaire au dechiffrage du message. (exemple : les coordonnées pour envoyer un missile nucléaire doivent être ultras-précises)

7.6.2 Protection contre les infections

Il faudra conserver les fichiers de maniere securisée et prudente ou alors les supprimer une fois que ce ceux-ci n'aient plus d'utilité.

7.7 Standards influençant le produit

7.7.1 Conformité avec des standards

Pour concevoir le projet, l'equipe de developpement s'est mis d'accord sur les conventions de codage a respecter.

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. Nous avons testé le site qui par exemple pour le dechiffrement avec Vigenere, fonctionne trés bien.
-Decrypto : disponible sur le Google Play Store et gratuit.
-Axcrypt : logiciel gratuit.
Des logiciels payants/privés existent surement a l'usage des professionnels ou encore des services de police spécialisés.

8.2 Nouveaux problèmes, créés par le nouveau système

Il peut y avoir un problème de place ou mémoire lors de l'installation du "systeme" malgré que l'application soit légère.

Un ralentissement de "l'environnement" peut aussi etre constaté a la suite de l'utilisation du nouveau système.

8.3 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 (ou service a livrer) est identifié. De plus, les contraintes a respecter sont evaluées et la strategie de realisation est mise en place.
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.

8.4 Contrôle final de qualité sur site (Cutover)

Controle final sur un texte test. Un texte chiffré par vigenere et par substitution seront preparés, ainsi que leurs versions dechiffrées. Le resultat de ceux-ci via l'utilisation de l'application sera comparé a celui resultat preparé "sur feuille"(résultat théorique).

8.5 Risques liés au projet

Avec l'utilisation de l'application, certains risques existent. En effet, une personne etrangère peut avoir accés a l'ordinateur et ainsi récupérer les fichiers decryptés telechargés ou les fichiers originals(avant cryptage).

8.6 Organigramme

Détails des modules :

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

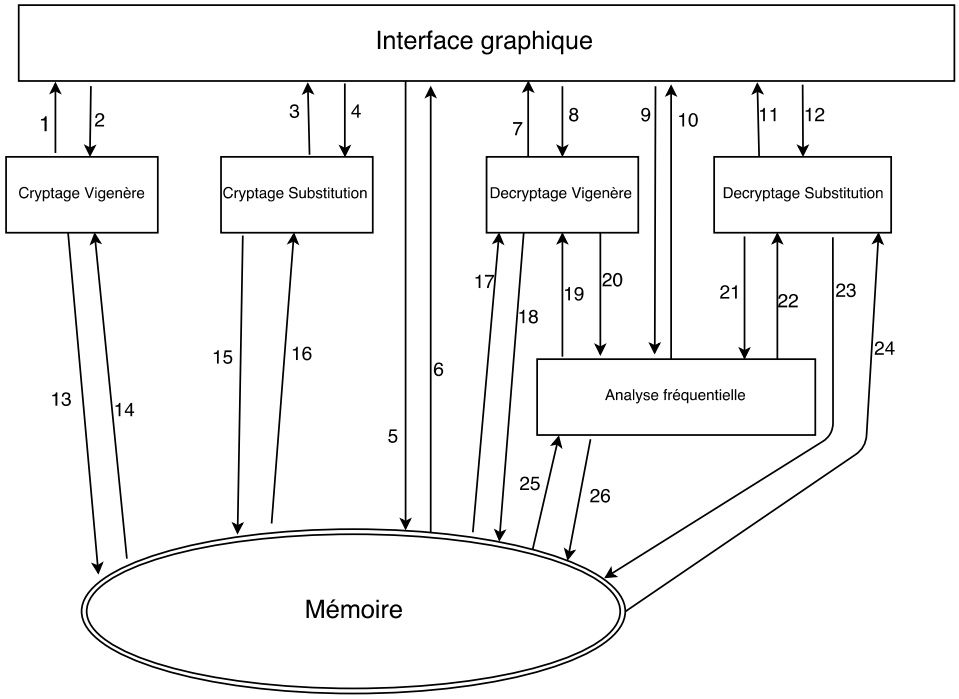
Decryptage Vigenère :
-decrypter le message

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



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

8.7 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	

8.8 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.

8.9 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.

8.10 Idées de solutions

Il s'agira de rentrer un nouveau tableau de données pour chaques nouvelles langues et pour chaque nouveau style. Au vu de l'agencement des caractères dans le texte, l'application pourra savoir automatiquement quelle operation le client cherche à effectuer (cryptage ou décryptage).

9 Conclusion

Notre application, qui permettra au client de manière simple de crypter ou decrypter des textes à l'aide de Vigenère ou du procédé de substitution, s'appelera Dcrypt.

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.