

# Cahier Des Charges

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

20 mars 2017

## 1 Preambule

Tout d'abord, nous allons parler de 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. Le mot steganographie vient du grec ancien 'steganós' qui veut dire "étanche" et 'graphein' qui signifie « écriture ». Exemples d'utilisation : encre invisible sur une feuille, 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), image(manipulation des indicateurs numeriques de couleurs RVB)..etc 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. Ce dernier vient des mots en grec ancien 'kruptos', signifiant "caché" et 'graphein' signifiant lui "écrire". Globalement, cela consiste à protéger des messages. 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 par un potier qui avait gravé sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots. C'est également une science nouvelle car elle est encore utilisée de nos jours dans plusieurs domaines tels que les banques(cartes), le web(navigateurs)..etc L'importance de la cryptologie se mesure par le faite qu'elle a été utilisée lors des deux guerres mondiales. Lors de la Premiere tout d'abord, où la maitrise cryptographique des francais les a avantagés par rapport a leurs ennemis. De plus, cela a même precipité l'entrée en guerre des Etats-Unis a cause du telegramme Zimmerman intercepté en 1917 par le Royaume-Uni. Selon certains spécialistes, les exploits des alliées en matière de cryptanalyse auraient permis d'écourter la guerre d'un a deux ans. Après les guerres, une nouvelle forme de cryptographie liée a l'ère de l'informatique est apparue.

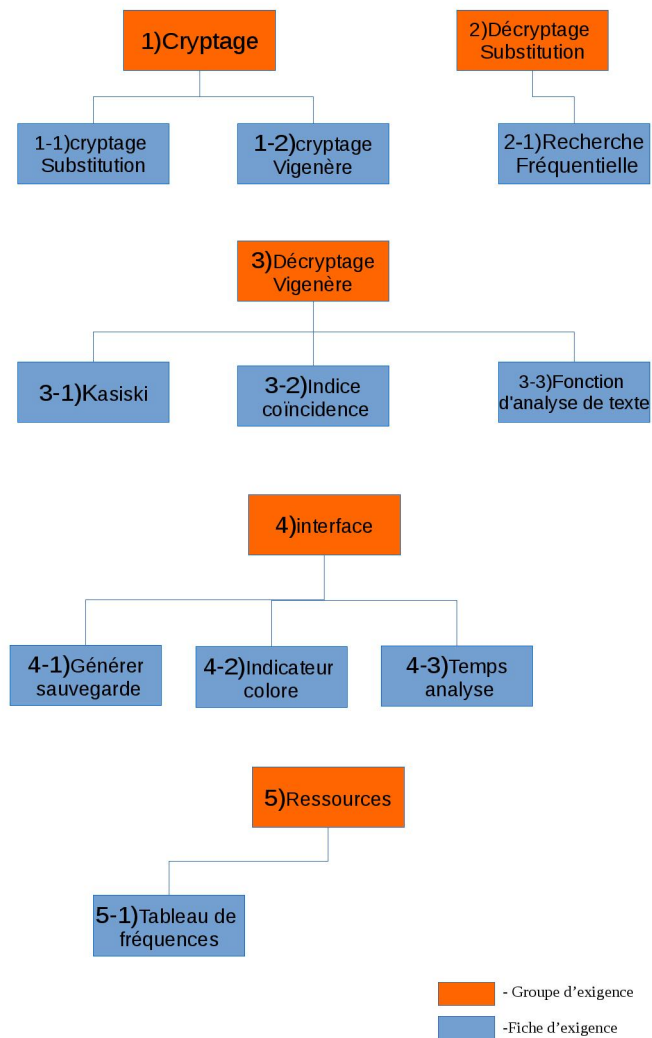
Ci-dessous un tableau récapitulatif résumant les différents chiffrements les plus connus :

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

## 2 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 notre travail.

#### 4.1.2 Objectif de la section

L'objectif de ce module est de nous apprendre a travailler en equipe pour 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 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 Maître d'ouvrage

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

## 4.3 Utilisateurs du produit

# 5 Contraintes sur le projet

## 5.1 Contraintes imposées non négociables

### 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 coïncidences pour déchiffrer par Vigenère.

### 5.1.3 Lieux de fonctionnement prévus

Il est préférable que l'utilisateur utilise un ordinateur moderne pour sa rapidité et sa fluidité.

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

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

### 5.1.5 Quel est le budget affecté au projet ?

Le client ne nous a pas référé son budget.

## 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

Les personnages Alice et Bob sont des figures classiques en cryptologie. Ces noms sont utilisés au lieu de « personne A » et « personne B » ; Alice et Bob cherchent dans la plupart des cas à communiquer de manière sécurisée. Alice est la personne qui envoie le message. Bob est celui qui veut recevoir le message. Oscar est celui qui essaye d'attaquer le message.

## 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 à ce que même un enfant puisse lancer le décryptage.

## 6 EXIGENCES FONCTIONNELLES

### 6.1 Portée du travail

#### 6.1.1 Situation actuelle

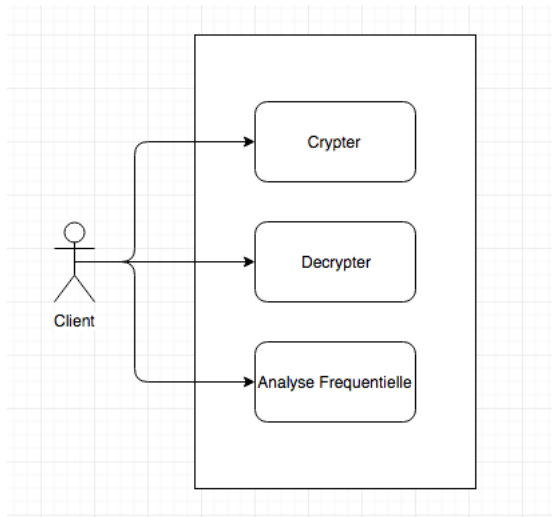
Nous n'avons aucune base pour notre application, nous allons la créer de toutes pièces.

#### 6.1.2 Contenu du travail

Il est nécessaire de connaître 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.

## 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 être utilisé par des personnes sans qu'elles y soient formées.

#### **7.2.2 Personnalisation et internationalisation**

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

#### **7.2.3 Facilité d'apprentissage**

Le développement 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.

#### **7.3.3 Fiabilité et disponibilité**

Le programme devrait être disponible pour une utilisation de 24 heures par jour et 365 jours par an.

### **7.4 Adéquation du produit avec son environnement**

#### **7.4.1 Environnement physique prévu**

Le programme sera utilisé sur un ordinateur.

#### **7.4.2 Environnement technologique prévu**

Le programme pourra fonctionner sur Windows, Linux et Mac.

#### **7.4.3 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 à 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 en matière de support**

L'utilisateur doit pouvoir communiquer avec d'autres utilisateurs et/ou les développeurs en charge de la maintenance.

#### **7.5.4 Exigences de portabilité**

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

#### **7.5.5 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**

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

#### **7.6.2 Protection des données à caractère personnel**

Message d'information à l'ouverture de l'application qui permet d'informer l'utilisateur des précautions à prendre.

#### **7.6.3 Audit et traçabilité**

Définition d'un répertoire de sauvegarde avec les dates des messages.

#### **7.6.4 Protection contre les infections**

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

## **7.7 Exigences culturelles et politiques**

### **7.7.1 Exigences culturelles**

L'application pourra gérer plusieurs langues (plusieurs tableaux de fréquences de lettres).

## **7.8 Lois et standards influençant le produit**

### **7.8.1 Conformité avec la loi**

Les informations personnelles seront soumises à la loi sur la protection des données personnelles (Loi informatique et libertés).

### **7.8.2 Conformité avec des standards**

La notion de conventions de codage (coding style) désigne un ensemble de règles et de conseils adoptés par les membres d'un projet logiciel pour écrire et mettre en forme du code. Les conventions de codage visent essentiellement à améliorer la lisibilité du code : elles doivent permettre au programmeur d'identifier « du premier coup d'œil » un maximum de choses dans le code, de se repérer facilement, de savoir où trouver les choses, etc. Une fois adoptées, elles facilitent grandement l'écriture, la maintenance et aident à éviter certaines erreurs. Dès lors qu'on travaille sur un projet logiciel d'une certaine ampleur, qui plus est à plusieurs, l'expérience montre qu'il est très important de se mettre d'accord sur les conventions de codage. Ainsi, nous avons décidé de définir nous même les règles à respecter durant le codage. Comme par exemple pour l'indentation, les noms des variables, les noms des fonctions, etc.

## **8 AUTRES ASPECTS DU PROJET**

### **8.1 Questions sans réponse**

Nous pensons avoir abordé une grande partie des aspects du projet et des attentes du client.

### **8.2 COTS : progiciels et composants commerciaux**

Il existe sur le marché pas mal de produits pouvant être des solutions potentielles/de remplacement. En effet, sur internet ("en ligne"), il existe des sites proposant de decrypter votre texte. Nous avons par exemple testé le site [www.dcode.fr](http://www.dcode.fr), qui pour le déchiffrement avec Vigenere, fonctionne très bien. Il y'a aussi une application (Decrypto) sur le Google Play Store (parmi plusieurs applis), qui est gratuite et qui permet aussi de déchiffrer Vigenere par exemple. Enfin, on peut télécharger des logiciels gratuits comme Axcrypt. Des logiciels payants/privés existent sûrement à l'usage des professionnels ou encore des services de police spécialisés.

### **8.3 Nouveaux problèmes, créés par le nouveau système**

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

-Un ralentissement de "l'environnement" peut aussi être constaté à la suite de l'utilisation du nouveau système.

### **8.4 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 à livrer) est identifié. De plus, les contraintes à respecter sont évaluées et la stratégie de réalisation est mise en place. Phase II : Définition du projet : Son contenu est défini de manière très précise et la planification des échéances et de la répartition du travail est établie. Phase III : Réalisation : On réalise le projet en adéquation avec les exigences du client et selon le plan de travail défini au préalable. Phase IV : Finalisation : Le produit est évalué puis remis au client.

## 8.5 Contrôle final de qualité sur site (Cutover)

Contrôle final sur un texte test. Un texte chiffré par vigenere et par substitution seront préparés, ainsi que leurs versions déchiffrées. Le résultat de ceux-ci via l'utilisation de l'application sera comparé à celui résultat préparé "sur feuille"(résultat théorique).

## 8.6 Risques liés au projet

Avec l'utilisation de l'application, certains risques existent. En effet, une personne étrangère peut avoir accès à l'ordinateur et ainsi récupérer les fichiers decryptés téléchargés ou les fichiers originaux( avant cryptage).

## 8.7 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 Français(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

Cryptage Substitution :

- créer une clé aléatoirement
- crypter le message

Cryptage Vigenère :

- crypter le message

Decryptage Substitution :

- decrypter le message

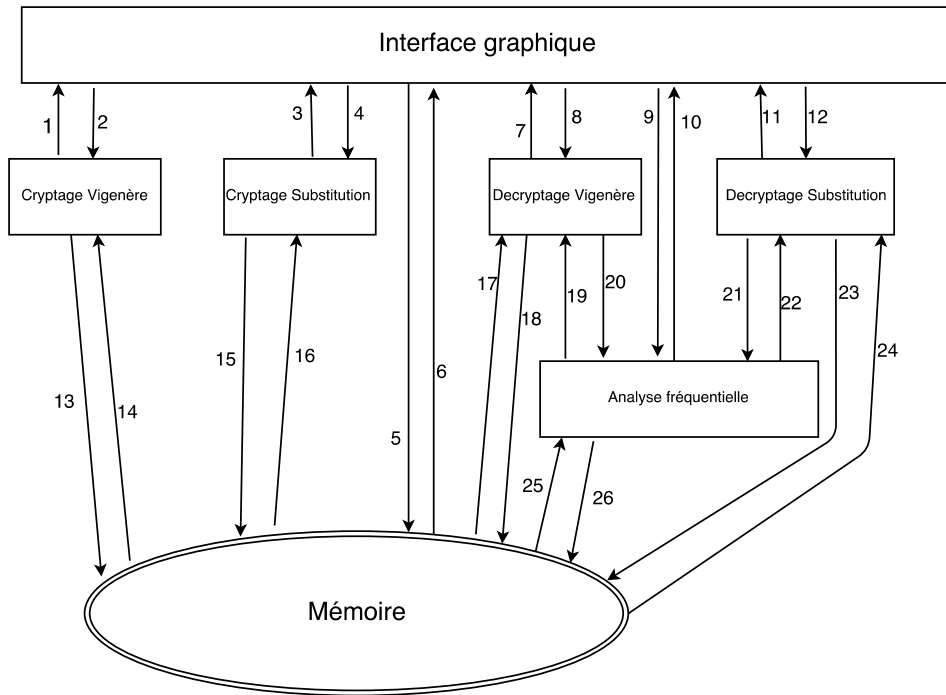
Analyse fréquentielle :

- analyse fréquentielle sur texte donné

Decryptage Vigenère :

- decrypter le message





- 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

## 8.8 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	

## 8.9 Manuel utilisateur et formations à envisager

L'utilisateur aura accès 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'à importer son texte.

## 8.10 Salle d'attente : idées pour les futures versions

Bien que le programme ait été demandé que pour la langue française et anglaise, il sera sans doute possible d'ajouter d'autres langues dans des versions futures. 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 à l'application de savoir directement si l'on va crypter ou décrypter un texte.

## 8.11 Idées de solutions

Il s'agira de rentrer un nouveau tableau de données pour chaque 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 décrypter des textes à l'aide de Vigenère ou du procédé de substitution, s'appellera Dcrypt.

Après l'analyse des besoins et après avoir constaté que la programmation orienté-objet n'était pas nécessaire, nous avons donc choisi d'utiliser le langage C. C'est en effet un langage procédurale et performant. De plus, toute l'équipe le maîtrise, entraînant ainsi une diminution des coûts liée à un éventuel 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 développement de notre application.