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 egalement 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 télegramme Zummerman 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

Numéro de l'exigence : 1	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Cryptage d'un texte	
Description : Utiliser le cryptage de Vigenère ainsi que le chiffrement par substitution.	
Justification : Permet d'avoir un texte crypté rapidement, facilite le décryptage	
Origine : Demande de développeur : Pouvoir obtenir un texte chiffré rapidement et ainsi vérifier le décryptage correct	
Critères de satisfaction : Crypter un texte afin d'obtenir un message crypté	
Contentement du maître d'ouvrage : 4	Mécontentement du maître d'ouvrage : 2
Exigences dépendantes : Fonction d'analyse du texte chiffrer. Tableau des fréquences de lettres(anglais, français).	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie*.	
Historique : Envisager après réflexion	

Numéro de l'exigence : 1.1	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Chiffrement par substitution	
Description : Utiliser le chiffrement par substitution.	
Justification : Permet d'avoir un texte crypté rapidement, facilite le décryptage	
Origine : Demande de développeur : Pouvoir obtenir un texte chiffré par substitution et ainsi vérifier le décryptage correct	
Critères de satisfaction : Crypter par substitution un texte afin d'obtenir un message crypté	
Contentement du maître d'ouvrage : 4	Mécontentement du maître d'ouvrage : 2
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Envisager après réflexion	

Numéro de l'exigence : 1.2	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Cryptage Vigenère.	
Description : Chiffrer un texte avec le chiffrement de Vigenère	
Justification : Permet d'obtenir des tableaux de fréquences nécessaires au déchiffrage d'un texte.	
Origine : Demande du développeur : Pouvoir chiffrer un texte encoder avec un chiffrement de Vigenère.	
Critères de satisfaction : Crypter un texte par Vigenère afin d'obtenir un texte chiffrer.	
Contentement du maître d'ouvrage : 4	Mécontentement du maitre d'ouvrage : 2
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Initial, présente depuis le début.	

Numéro de l'exigence : 2	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Décryptage texte chiffrer par substitution	
Description : Utiliser la recherche fréquentielle pour la cryptanalyse d'un texte chiffré	
Justification : Cet outil est le plus efficace pour le déchiffrage d'un texte utilisant le chiffrement par substitution	
Origine : Demande du client : Pouvoir déchiffrer un texte encoder avec un chiffrement par substitution.	
Critères de satisfaction : Pouvoir décrypter une partie d'un texte chiffré par substitution afin d'obtenir un texte compréhensible.	
Contentement du maître d'ouvrage : 5	Mécontentement du maître d'ouvrage : 5
Exigences dépendantes : 2.2	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Initial, présente depuis le début.	

Numéro de l'exigence : 2.1	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Faire une recherche fréquentielle pour le déchiffrage par substitution	
Description : Utiliser la recherche fréquentielle pour la cryptanalyse d'un texte chiffré.	
Justification : Permet de retrouver certaines lettre du texte chiffré par recherche fréquentielle.	
Origine : Demande du développeur : Cet outil est le plus efficace pour la cryptanalyse d'un chiffrement par substitution	
Critères de satisfaction : Retrouver une bonne partie du texte chiffré à l'aide de cet outil	
Contentement du maître d’ouvrage : 5	Mécontentement du maître d'ouvrage : 5
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Initial, présente depuis le début.	

Numéro de l'exigence : 3	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Décryptage texte chiffrer en Vigenère	
Description : Utiliser le test de Kasiski et l'indice de coïncidence pour la cryptanalyse du texte chiffrer.	
Justification : Ces deux outils sont les plus efficaces pour le déchiffrage d'un texte utilisant le chiffrement de Vigenère	
Origine : Demande du client : Pouvoir dechiffrer un texte encoder avec un chiffrement de Vigenère.	
Critères de satisfaction : Décrypter une partie d'un texte par Vigenère afin d'obtenir un texte compréhensible.	
Contentement du maître d'ouvrage : 5	Mécontentement du maitre d'ouvrage : 5
Exigences dépendantes : 3.1 - 3.2 – 3.3 – 5.2	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Initial, présente depuis le début.	

Numéro de l'exigence : 3.1	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Test de Kasiski	
Description : Utiliser le test de Kasiski pour connaître la taille du mot clef.	
Justification : Ce test permet d'obtenir une conjecture fiable sur la taille du mot clef.	
Origine : Demande du développeur : outil nécessaire pour la cryptanalyse.	
Critères de satisfaction : Coder soit même un texte avec une clef connu et voir si la conjecture est correct.	
Contentement du maître d'ouvrage : 5	Mécontentement du maitre d'ouvrage : 5
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Découverte après recherche.	

Numéro de l'exigence : 3.2	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Indice de coïncidence	
Description : Utiliser l'indice de coïncidence pour trouver les valeurs des caractères composant le mot clef.	
Justification : Cette indice permet de retrouver efficacement le mot clef.	
Origine : Demande du développeur : outil nécessaire pour la cryptanalyse	
Critères de satisfaction : Coder soit même un texte avec une clef connu et voir si la conjecture est correct.	
Contentement du maître d'ouvrage : 5	Mécontentement du maitre d'ouvrage : 5
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Découverte après recherche.	

Numéro de l'exigence : 3.3	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Fonction d'analyse de texte	
Description : Calcul la fréquence d'apparition moyenne de chaque lettres et paires de lettres consécutives.	
Justification : Permet d'obtenir des tableaux de fréquences nécessaires au déchiffrage d'un texte.	
Origine : Demande du développeur : outil nécessaire pour la cryptanalyse	
Critères de satisfaction : Calculer manuellement le fréquence d'un texte afin de pouvoir lancer la fonction d'analyse et comparer les résultats.	
Contentement du maître d'ouvrage : 5	Mécontentement du maitre d'ouvrage : 5
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Douglas Stinson, *Cryptographie.*	
Historique : Initial, présente depuis le début.	

Numéro de l'exigence : 4	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Interface graphique	
Description : L'interface pour le client durant le décryptage d'un texte.	
Justification : Faire une interface afin d'afficher le résultat à l'utilisateur.	
Origine : Demande du développeur : L'interface doit être facile d'utilisation pour tous.	
Critères de satisfaction : Pouvoir afficher des informations à l'écran de l'utilisateur.	
Contentement du maître d'ouvrage : 5	Mécontentement du maître d'ouvrage : 5
Exigences dépendantes : 4.1 – 4.2 – 4.3 – 4.4	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Initial, présente depuis le début.	

Numéro de l'exigence : 4.1	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Générer un fichier de sauvegarde	
Description : Génère un fichier de sauvegarde une fois le décryptage fini.	
Justification : Permet de conserver une copie du décryptage.	
Origine : Demande du développeur : La sauvegarde d'un texte décrypter faciliterais le client	
Critères de satisfaction : Pouvoir sauvegarder le texte exacte du décryptage.	
Contentement du maître d'ouvrage : 4	Mécontentement du maître d'ouvrage : 3
Exigences dépendantes : 2 - 3	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Envisager après réflexion	

Numéro de l'exigence : 4.2	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Indicateurs colorés	
Description : Mettre en relief avec des couleurs les digrammes et trigrammes qui se répètent dans le texte et qui sont très peu fréquent dans la langue d'origine du texte attaquer.	
Justification : Permet d'obtenir une interface simple et efficace.	
Origine : Demande du développeur pour aider l'utilisateur.	
Critères de satisfaction : Attribuer une couleur spécifique a certains caractères.	
Contentement du maître d'ouvrage : 3	Mécontentement du maitre d'ouvrage : 1
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Envisager après réflexion	

Numéro de l'exigence : 4.3	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Temps pour analyse	
Description : Donner une approximation du temps nécessaire a l'utilisateur pour attaquer le texte chiffrer.	
Justification : Permet d'obtenir un indicateur visuel utile a l'utilisateur.	
Origine : Demande du développeur pour aider l'utilisateur.	
Critères de satisfaction : Obtenir une estimation du temps nécessaire a l'utilisateur pour déchiffrer un texte.	
Contentement du maître d'ouvrage : 2	Mécontentement du maitre d'ouvrage : 1
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Envisager après réflexion.	

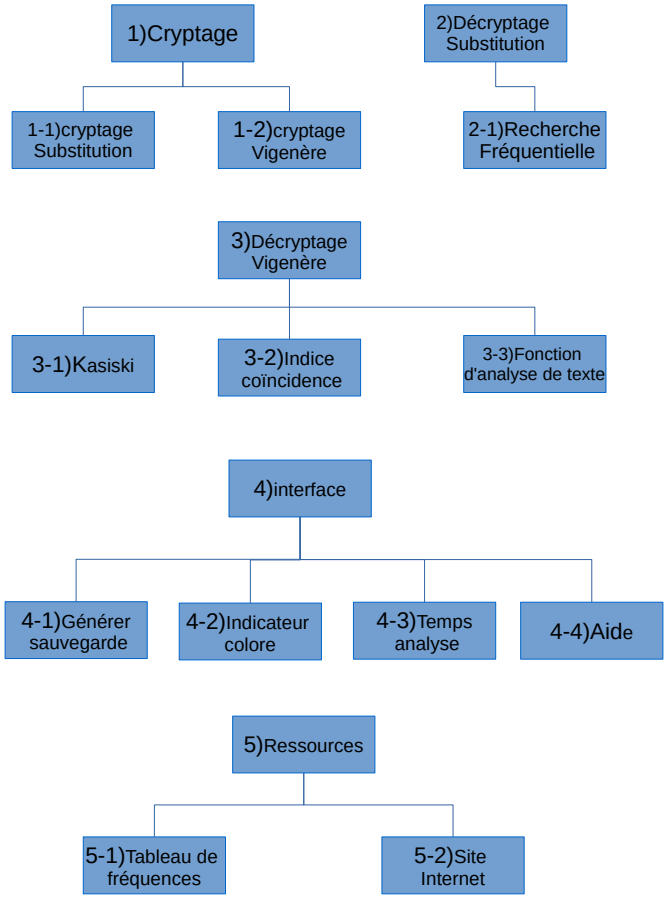
Numéro de l'exigence : 4.4	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Aide au décryptage.	
Description : Afficher des commentaires/bulles d'aides pour orienter l'utilisateur dans le déchiffrage d'un texte.	
Justification : Permet d'aider l'utilisateur a prendre les bonnes décisions.	
Origine : Demande du développeur pour aider l'utilisateur.	
Critères de satisfaction : Avoir des bulles/commentaires informe l'utilisateur des choix a prendre.	
Contentement du maître d'ouvrage : 2	Mécontentement du maître d'ouvrage : 1
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Envisager après réflexion.	

Numéro de l'exigence : 5	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Ressources	
Description : Rassembler toutes les ressources en rapport avec notre application (ex : site internet, bibliographie, ..).	
Justification : Centraliser les ressources utile/utiliser.	
Origine : Demande du développeur : organisation.	
Critères de satisfaction : Avoir un historique complet et des informations sur le site.	
Contentement du maître d'ouvrage : 4	Mécontentement du maitre d'ouvrage : 3
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Site internet (www..exemple.fr)	
Historique : Envisager après réflexion.	

Numéro de l'exigence : 5.1	Type d'exigence : Fonctionnelle
Événement/Cas d'utilisation : Tableaux des fréquences des lettres.	
Description : Utiliser un tableau des fréquences des lettres pour décrypter une chiffrement de Vigenère.	
Justification : Besoin d'un tableau contenant les fréquences d'apparition des lettres de l'alphabet dans une langue.	
Origine : Demande du développeur : L'utilisation de ce tableaux est essentielle au décryptage.	
Critères de satisfaction : Obtenir ce tableaux dans les différents langages(anglais, français)	
Contentement du maître d'ouvrage : 5	Mécontentement du maître d'ouvrage : 5
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Découverte après recherche	

Numéro de l'exigence : 5.2	Type d'exigence : Non Fonctionnelle
Événement/Cas d'utilisation : Site internet.	
Description : Développer un site internet contenant toute les information de la futur application.	
Justification : Facilités pour l'utilisateur de bien comprendre l'application.	
Origine : Demande du développeur : Développer un « Readme » sous forme de site internet.	
Critères de satisfaction : Obtenir ce tableaux dans les différents langages(anglais, français)	
Contentement du maître d'ouvrage : 3	Mécontentement du maître d'ouvrage : 1
Exigences dépendantes : Aucune	Exigences conflictuelles : Aucune
Document relatifs : Aucun	
Historique : Envisager après réflexion	

3 Numerotation des exigences


1)Cryptage
2)Décryptage Substitution
1-1)cryptage Substitution
1-2)cryptage Vigenère
2-1)Recherche Fréquentielle
3)Décryptage Vigenère
3-1)Kasiski
3-2)Indice coïncidence
3-3)Fonction d'analyse de texte
4)interface
4-1)Générer sauvegarde
4-2)Indicateur colore
4-3)Temps analyse
4-4)Aide
5)Ressources
5-1)Tableau de fréquences
5-2)Site Internet

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 etre 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.

4.3 Utilisateurs du produit

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 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 a ce que même un enfant puisse lancer le décryptage.

6 EXIGENCES FONCTIONNELLES

6.1 Portée du travail

6.1.1 Situation actuelle

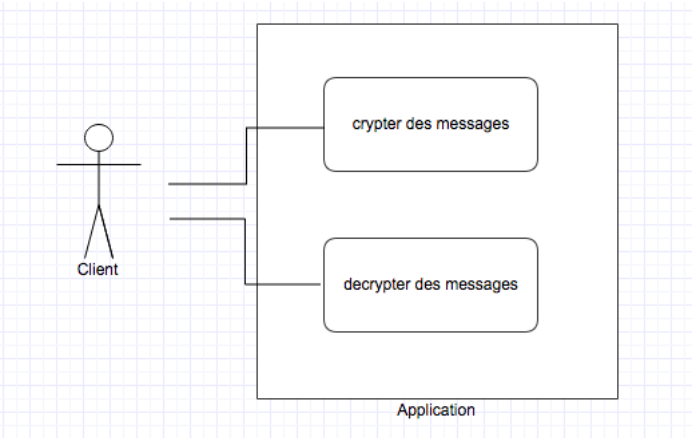
Nous n'avons aucune base pour notre application, nous allons la créer de toutes pièces.

6.1.2 Contenu du travail

Il est nécessaire de 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 methodes 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 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.

7.3.3 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 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 en matière de support

L'utilisateur doit pouvoir communiquer avec d'autres utilisateurs et/ou les developpeurs 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 a 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

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 des données à caractère personnel

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

7.6.3 Audit et traçabilité

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

7.6.4 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 Exigences culturelles et politiques

7.7.1 Exigences culturelles

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

7.8 Lois et standards influençant le produit

7.8.1 Conformité avec la loi

Les informations personnelles seront soumises a 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 ou trouver les choses, etc.Une fois adoptés, 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 a 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 etre 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, qui pour le dechiffrement avec Vigenere, fonctionne trés bien. Il y'a aussi une application (Decrypto) sur le Google Play Store (parmi plusieurs applis),qui est gratuite et qui permet aussi de dechiffrer Vigenere par exemple. Enfin, on peut telecharger des logiciels gratuits comme Axcrypt. Des logiciels payants/privés existent surement a 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 "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.

8.4 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 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.

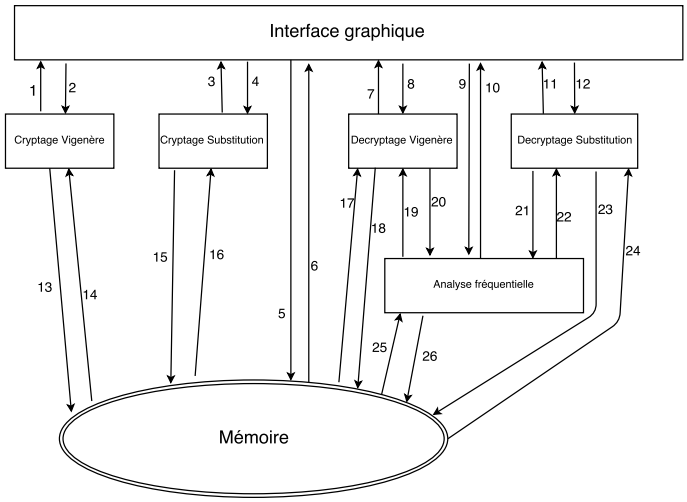
8.5 Contrôle final de qualité sur site (Cutover)

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"(resultat theorique).

8.6 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 recuperer les fichiers decryptés telechargés ou les fichiers originals(avannt cryptage).

8.7 Organigramme


Interface graphique
Cryptage Vigenère
Cryptage Substitution
Decryptage Vigenère
Decryptage Substitution
Analyse fréquentielle
Mémoire
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

Détails des flèches :
1 un ensemble de données contenant le texte crypté 2 un nom du fichier 3 un ensemble de données contenant le texte crypté 4 un nom du fichier 5 un nom du fichier 6 fichier texte : clair , crypter ,decrypter ou analyse frequentielle 7 un ensemble de donnees contenant le texte en clair 8 un nom du fichier 9 un ensemble de données contenant l'analyse frequentielle 10 un nom du fichier 11 un ensemble de données contenant le texte decrypté ou le texte clair 12 un nom du fichier 13 un nom du fichier 14 fichier texte clair 15 un nom du fichier 16 fichier texte clair 17 un fichier texte crypté 18 un nom du fichier 19 un ensemble de données contenant l'analyse frequentielle 20 un nom du fichier 21 un nom du fichier 22 un ensemble de données contenant l'analyse frequentielle 23 un nom du fichier 24 un fichier texte crypté 25 un fichier texte en crypté ou en clair 26 un ensemble de donnees contenant l'analyse frequentielle

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

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

Decryptage Vigenère : -decrypter le message

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	500	Benyamna & Capdenat
Total	1000	

8.9 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.

8.10 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.

8.11 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

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 couts 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.