Cahier Des Charges

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

7 mars 2017

1 Preambule

Tout d'abord, nous allons parler de la steganographie, qui est "l'ancetre" 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 'graphe' 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 proteger des messages. En effet, comme le dit Ronald Rivest, grand cryptologue americain 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 La cryptologie était 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. Pendant la Seconde, le chiffre Enigma etait utilisé tout comme le chiffre Lorenz, mais il n'a jamais été cassé. Ainsi, des chiffreurs ont été utilisés de meme que des bombes afin de connaitre la clé quotidienne de certains jours pour attaquer les messages.

2 fiche d'exigence

3 numerotation des exigences

4 fondament du projet

4.1 But Du Projet

4.1.1 Probleme 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/professeur va evaluer 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 realiser un automayique d'aide au décryptage, capable de retrouver une grande partie du texte d'origin a partir d'un texte chiffré. Il devra etre capable de déchiffré le chiffrement de vignère 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 annee d'info dirigé par Mme Kloul qui travaille pour 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, décrypter un chiffrement de Vignère 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 vigenère le message.

5.1.3 Lieux de fonctionnement prévus

Le produit étant une application, il faudra un ordinateur afin de le lancer. 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

Cette section donne les définitions de tous les termes et acronymes utilisés dans le projet.

k est la clé

m est la taille de la clé

n est la taille de 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

Exigences NON FONCTIONNELLE -Le developpement d'un site web présentant le produit ainsi que toutes ces carectéristiques. Ce site web pourra également disposer d'un forum permettant aux internautes de proposer certaines amélioration à faire sur l'application et également critiquer certaines fonctionnalités de l'application.

-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 la situation actuelle

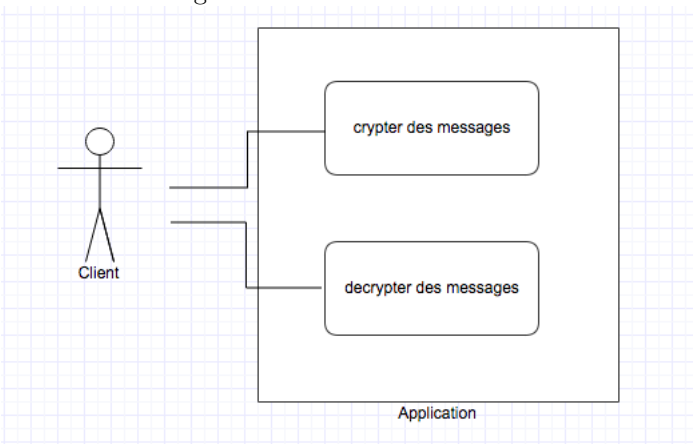
pour l'instant cette application n'existe pas encore donc il ne sagit pas d'une amelioration

6.1.2 contenu du travail

il est nessaissaire de connaitre le cryptage et le decryptage avec le code de vigenere et la methode de substitution

6.2 Portée du produit : cas d'utilisation

subsub le diagramme de cas d'utilisation



subsub description de ce diagramme dans cette application il n'ya qu'un seul type d'utilisateur qui est le client et qui peut crypter et decrypter avec deux methode differentes

6.3 Exigences fonctionnelles et exigences sur les données

subsub Exigences fonctionnelles je crois quil faut mettre les numeros des exigences fonctionnelles (pas sur) subsub Exigences sur les données

7 EXIGENCES NON FONCTIONNELLES

7.1 Ergonomie et convivialité du produit

a.l'interface L'interface permettera de rentrer facilement le texte à décrypter, par copier coller par exemple. L'interface permettera de choisir la langue (anglais, français) grâce à un simple menu déroulant. L'interface permettera d'afficher facilement le resultat obtenu. b.Le style du produit le programme sera évaluer par la résponsable du module Projet de la L3 donc il doit apparaître simple et effiace (pas de superflu). Le programme ne doit pas etre trop gros en terme de resolution, on doit pouvoir l'afficher sur tous les types d'écran d'ordinateur.

7.2 Facilité d'utilisation et facteurs humains

a.facilité d'utilisation Le programme sera simple à utiliser pour un adulte. Le programme aidera l'utilisateur en cas de mauvaise utilisation (fenetre warnning si vous lancer une analyse fréquentielle sur un cryptage de vignere il vous proposera d'utiliser le drecryptage adéquats) Le programme pourra etre utilisé par des personnes sans qu'ils y soient formés. Sur 100 utilisations le programme devra avoir un taux inférieure à Xb.Personnalisation et internationalisation Le programme sera trop simple pour etre personnalisable et il sera en anglais. c.Facilité d'apprentissage Il sera possible au grand public d'utiliser le programme sans formation. d.facilité d' compréhension et politesse Le produit devrait utiliser des symboles et des mots naturellement compréhensibles par les utilisateurs potentiels. Le produit doit cacher les détails de sa construction à l'utilisateur. e.Exigence d'accessibilité A voir avec les autres

7.3 Fonctionnement du produit

a.Rapidité d'exécution et temps de latence La réponse sera assez rapide pour éviter d'interrompre le flux de pensée de l'utilisateur. b. Exigences critiques de sûreté c. 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 resultats du décryptage. d. Fiabilité et disponibilité Le programme devrait être disponible pour une utilisation de 24 heures par jour et 365 jours par an. e. Robustesse ou tolérance à un emploi erroné f. Capacité de

stockage et montée en charge Le programme ne pourra pas stocker des données. g. Adaptation du produit à une augmentation de volume à traiter h. Longévité

7.4 Adéquation du produit avec son environnement

a. Environnement physique prévu Le programme sera utilisé sur un ordinateur. b. Environnement technologique prévu Le programme pourra fonctionner sur Windows et Linux (MAC ?) c. Applications « partenaires » (avec lesquelles le produit doit collaborer) d. 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

a. 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/bugs. (test unitaire, indicateurs comme des variables, outils de debugs comme valgrind) ;.. b. 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. Demande d'aides au developpeur charger de la maintenance de l'application. c. Exigences en matière de support L'utilisateur doit pouvoir communiquer avec d'autres utilisateurs et/ou les developpeurs en charge de la maintenance. d. Exigences de portabilité L'application peut fonctionner sur plusieurs environnements car "un makefile est fournis et permet a l'utilisateur de buid en fonction de son environnement linux/windows/.. e. Installation du système L'application doit pouvoir être installer très facilement sur n'importe quel environnement. Le site internet doit permettre de repondre a certaines interrogations.

7.6 Sécurité

a. Accès au système Besoin d'un mot de passe pour consulter le message en clair (l'application ayant déja enregistrer les clefs(donnees sensibles)). ? - ¿ Definition de deux profils pour utiliser l'application ? b. Intégrité Definition d'un niveau d'importance de "l'exactitude" necessaire au dechiffrage du message. (exemple : les coordonnées pour envoyer un missile nucleaire doivent etre ultra precise)/ c. Protection des données à caractère personnel Message d'information a l'ouverture de l'application qui permet d'informer l'utilisateur de ses droits/devoirs. d. Audit et traçabilité Definition d'un repertoire de sauvegarde avec les dates des messages. e. Protection contre les infections Hacher les textes sauvegarder afin de proteger l'utilisateur d'une attaque informatique.

7.7 Exigences culturelles et politiques

a. Exigences culturelles L'application pourra gerer plusieurs langues (plusieurs tableaux de frequencages de lettres) b. Exigence politiques L'application et notamment les informations obtenue via l'application devront être hermétique vis a vis de n'importe quel états/organisation.

7.8 Lois et standards influençant le produit

a. Conformité avec la loi Les informations personnelles seront soumis a la loi sur la protection des données personnelles (la loi informatique et libertés) b. Conformité avec des standards "on utilise un standard ?"

8 AUTRES ASPECTS DU PROJET

8.1 Questions sans réponse

Nous pensons avoir abordé la totalité des aspects du projet et repondu a toutes les 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 tester 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 existe surement a l'usage des professionnels ou encore des services de police.

8.3 Nouveaux problèmes, créés par le nouveau système

-pb de place/mémoire (appli lourde) -virus -ralentissement de "l'environnement"

8.4 Tâches à faire pour livrer le système

phases de developpement de l'appli ?

8.5 Contrôle final de qualité sur site (Cutover)

controle final sur un texte test

8.6 Risques liés au projet

8.7 Estimation des coûts du projet

Pour une estimation precise des coûts du projet il faut estimer le coût en taille, le coût en charge de travail, le coût des délais et le prix. Dans ce projet on vas surtout se concentrer sur la taille de l'application et donc détérminer son coût grace au nombre de lignes de code (que l'on ne pouras détérminer qu'aprés avoir réfléchis sur l'architecture du programme).

8.8 Manuel utilisateur et formations à envisager

L'utilisateur aura acces à un menu lui permettant de choisir de crypter ou décrypter un texte, puis la méthode qu'il veut utiliser pour ce faire (vignaire 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 les langues francaise et anglaise, il sera sans doute possible d'ajouter d'autre langues dans des versions futurs. Il pourras étre également possible d'ajouter une option permettant à l'utilisateur d'entrer un type de texte (poéme, roman, ordre militaire,...) pouvant aider au décryptage.

8.10 Idées de solutions

Il s'agiras de rentrer un nouvaux tableau de données pour chaque nouvelles langues et pour chaque nouveau style.