Cahier Des Charges

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

5 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 definition utilisee dans ce modele

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 fondament du projet

5.1 But Du Projet

5.1.1 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.

5.1.2 objectif de la section

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

5.1.3 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.

5.2 personnes et organismes impliqués dans les enjeux du projet

5.2.1 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.

5.3 utilisateurs du produit

6 contraintes sur le projet

6.1 contraintes imposees non negociables

6.1.1 contraintes sur la conseption de la solution

-Le produit doit permettre à l'utilisateur de décrypter une partie d'un message crypté.

-Le produit doit décrypter un chiffrement de Vignère et un chiffrement par substitution

-Toutes les deadlines concernant l'application et son cahier des charges doivent être respectées

6.1.2 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 le message.

6.1.3 Applications « partenaires » (avec lesquelles le produit doit collaborer)

Aucun partenaires nécessaires pour le moment.

6.1.4 « COTS » : Progiciels ou composants commerciaux

Aucun progiciels ou composants commerciaux imposés dans le projet.

6.1.5 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

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

La deadline pour les développeurs est le

6.1.7 Quel est le budget affecté au projet ?

Le client ne nous a pas référé son budget.

6.2 Glossaire et conventions de dénomination

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

k est la clé

n est la taille de la clé

m est la taille de message chiffré

6.3 Faits et hypothèses utiles

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

-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.

6.3.2 Hypothèses que l'équipe fait sur le projet

7 EXIGENCES FONCTIONNELLES

7.1 Portée du travail

7.1.1 la situation actuelle

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

7.1.2 contenu du travail

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

7.1.3 division du travail en évènnement metier

7.2 Portée du produit : cas d'utilisation

subsub le diagramme de cas d'utilisation le client , crypter , decrypter , et quoi d'autre ? subsub description de ce diagramme

7.3 Exigences fonctionnelles et exigences sur les données

8 EXIGENCES NON FONCTIONNELLES

8.1 Ergonomie et convivialité du produit

8.2 Facilité d'utilisation et facteurs humains

8.3 Fonctionnement du produit

8.4 Adéquation du produit avec son environnement

8.5 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.

8.6 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.

8.7 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.

8.8 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 ?"

9 AUTRES ASPECTS DU PROJET

9.1 Questions sans réponse

9.2 COTS : progiciels et composants commerciaux

9.3 Nouveaux problèmes, créés par le nouveau système

9.4 Tâches à faire pour livrer le système

9.5 Contrôle final de qualité sur site (Cutover)

9.6 Risques liés au projet

9.7 Estimation des coûts du projet

9.8 Manuel utilisateur et formations à envisager

9.9 Salle d'attente : idées pour les futures versions

9.10 Idées de solutions