Cahier Des Charges

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

28 février 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

6.1.2 Environnement de fonctionnement du système actuel

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

6.1.4 « COTS » : Progiciels ou composants commerciaux

6.1.5 Lieux de fonctionnement prévus

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

6.1.7 Quel est le budget affecté au projet ?

6.2 Glossaire et conventions de dénomination

6.3 Faits et hypothèses utiles

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

6.3.2 Hypothèses que l'équipe fait sur le projet