ESI Ãcole nationale SupÃ©rieure d'Informatique

Rapport

Cryptage et décryptage de fichier texte

Module : SFSD

Réalisé par :

Abchiche Sarah

Slimani Wassila Maria

Introduction

Le chiffrement ou cryptage est un procédé de [cryptographie](https://fr.wikipedia.org/wiki/Cryptographie) grâce auquel on a la possibilité de rendre la compréhension d’un document impossible à toute personne qui n'a pas la [méthode de (dé)chiffrement](https://fr.wikipedia.org/wiki/Cl%C3%A9_de_chiffrement). Ce principe est généralement lié au principe d'[accès](https://fr.wikipedia.org/wiki/Contr%C3%B4le_d%27acc%C3%A8s) conditionnel.

Méthode de cryptage (Le Non logique) :

Cette méthode est un système de cryptage basique mais pas trop limité. Le NON est un opérateur logique qui correspond à un "~" en langage C c’est un opérande qui peut avoir la valeur VRAI ou FAUX, il associe un résultat qui a lui-même la valeur inverse de celle de l'opérande d’origine.

En informatique, chaque caractère du message à coder est représenté par un entier, le code ASCII. Ce nombre est lui-même représenté en mémoire comme un nombre binaire à 8 chiffres (les bits).

Pour crypter un fichier donné, on effectue un inversement (Non logique), bit par bit. Le résultat en binaire peut être reconverti en caractères ASCII, puis on l’additionne avec la clé en faisant le modulo Le résultat donne alors le code ascii du caractère codé.

Pour décrypter, l'algorithme est complètement symétrique : pour avoir le message initial à partir du message codé, on soustrait la clé du caractère codé en faisant le modulo puis on effectue un NON logique bit à bit, le résultat en binaire sera convertie en caractère ASCII.