Simulation graphique de la machine Enigma I

Hakim Boulahya

Université Libre de Bruxelles, Belgique
hboulahy@ulb.ac.be

Abstract

Introduction

Dans le cadre d'un projet transdiscplinaire, il m'a été demandé d'implémenter un simulateur graphique de la machine Enigma I. Cette machine eletro-mécanique a été utilisé par l'armée Nazi durant la deuxième guerre mondiale. Elle a permis aux militaires Allemands de maintenir une communication secrète durant une majeur partie de la guerre. Très peu de machine ont survécu du au fait que les Alliés ont recu l'ordre de detruire toute machine enigma trouvé. nombre de possibilté cracké par Alan Turring donc pas secu

Contexte

Le chiffrement

Le chiffrement est un moyen de transformé une suite de caractère, en un autre suite, de telle sorte que cette dernière soit codé *i.e.* indéchiffrable sans une manipulation particulière (MCE). Cette action s'effectue généarelement à l'aide d'une clé de codage.

Imaginons un cas ou un individu A souhaite envoyer un message codé à un individu B. Pour cela il est nécessaire que les deux parties se communiquent une clé privé, *i.e.* que seule eux puissent en avoir la connaissance. Après l'échange des clés l'individu A peut chiffrer son message via un algorithme de codage et envoyer le message codé sur le canal de communication.

Soit f une fonction représentant l'algorithme de codage, k une clé privée et x un message. Le chiffrement du message peut être representé par l'équation:

$$f(x, k) = y$$

L'objectif de la fonction de chiffrement est de produire une sortie y. Cette sortie y ne doit pas représenter le contenu du message. C'est celle-ci qui sera envoyée à l'individu B. Lors de sa réception l'individu B devra effectuer la même action pour déchiffrer le message *i.e.* exécuter l'algorithme sur le message reçu pour en récupérer le message compréhensible. Ainsi l'équation suivante peut représenter le déchiffrement:

$$f(y, k) = x$$

Il est primordial que la clé de chiffrement ne soit pas divulger sur le canal de communication pour que le chiffrement et le déchiffrement ne soit applicable que par les parties concernées.

La machine Enigma I

La machine enigma est une appareil electro-mécanique de chiffrement utilisée durant la seconde guerre mondiale par l'armée nazi. Il en existe de plusieurs types tous utilisé à différentes périodes. Dans ce document nous nous interesseront uniquement à la machine Enigma `I`, également appelé *Ch.11a* par son constructeur. L'objectif de la machine est de produire un chiffrement pseudo-aléatoire d'un *input* - un caractère alphabétique latin - donnée[REFVERSARTICLE].

Etat de l'art

Le simulateur graphique

Conclusion

References