Simulation graphique de la machine Enigma I

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

Abstract

Cet article discute d'un simulateur de la machine Enigma `I`, une machine de cryptographie du 20ème siècle. L'objectif est de présenter un simulateur de cette machine composée d'une partie utilitaire et une partie graphique. La partie utilitaire à pour but d'aider au mieux à l'utilisation de l'algorithme de la machine tandis que la partie graphique s'oriente vers une simulation des composants de la machine. Dans cet article nous discutons du type de chiffrement qu'utilise Enigma ainsi qu'une présentation du simulateur que nous proposons.

Introduction

Dans le cadre du projet transdisciplinaire, il m'a été demandé de développer un simulateur graphique de la machine Enigma `I` en utilisant les technologies web `JavaScript`, `HTML5` et `CSS3`. La machine Enigma est un outil éléctromécanique de chiffrement utilisé durant la seconde guerre mondiale, majoritairement par l'armée nazi.

Le principal objectif du développement de cette simulation est de proposer à tous la possibilité d'utiliser une machine Enigma. En effet, très peu de vrai machine sont accessible. Plusieurs simulateurs de cette machine existe sur le web ou sous forme d'application bureau. Notre simulateur n'apporte pas de nouveauté dans le domaine de la cryptographie et à pour but uniquement d'apporter une autre vision de la simulation de la machine et d'offrir un accès au chiffrement que réalise cette machine à toute personne le désirant. Etant accessible sur le web, il est possible d'utiliser le simulateur Boulahya (2016) sur n'importe quelle appareil muni d'un navigateur web et d'une connexion Internet.

Dans cet article plusieurs sujets sont abordés: une brève introduction sur les algorithmes de chiffrement ainsi qu'une introduction sur le fonctionnement basique d'un type de ces algorithmes, une déscription de la machine Enigma `I` ainsi que son fonctionnement, un état de l'art des simulateurs d'Enigma les plus pertinents ainsi qu'une présentation du simulateur développé et du fonctionnement de celui-ci.

Contexte

Notation

Dans la suite du document, plusieurs notations sont utilisées:

- M = Un message à chiffrer
- K = Un clé secrète
- E = Une fonction de chiffrement
- D = Une fonction de déchiffrement
- C = Un message chiffré = E(M, K)

Le chiffrement

Le chiffrement est un moyen de transformer une suite de caractère, en une autre suite, de telle sorte que cette dernière soit codée *i.e.* indéchiffrable sans une manipulation particulière The McGraw-Hill Companies (2016). Cette action s'effectue généralement à l'aide de clés de chiffrement.

Il existe plusieurs types d'algorithme de chiffrement à clé: les algorithmes de clé asymétrique et les algorithmes de clé symétrique. Ici nous nous intéressons uniquement aux algorithmes de clé symétrique.

Les algorithmes de clé symétrique sont des algorithmes de chiffrement qui utilise une même clé pour chiffrer et déchiffrer un message Priyadarshini Patil (2015).

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 privée, *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 chiffrement à clé symétrique et envoyer le message chiffré sur le canal de communication.

Le chiffrement du message peut être representé par l'équation:

$$C = E(M, K)$$

L'objectif de la fonction de chiffrement est de produire une sortie C. Cette sortie C 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 l'action inverse pour déchiffrer le message *i.e.* exécuter l'algorithme de déchiffrement sur le message reçu pour en récupérer le message compréhensible. Ainsi l'équation suivante peut représenter le déchiffrement:

$$M = D(C, K) = D(E(C, K), K)$$

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.

Il existe différentes implémentations d'algorithme de chiffrement à clé symétrique. Les plus connus sont `AES` et `3DES` Priyadarshini Patil (2015). L'`AES` utilise des clés de tailles de 128, 192 ou 256 bits. Plus la tailles de la clé est grande plus les étapes de chiffrement sont élevés Priyadarshini Patil (2015).

La machine Enigma I

La machine Enigma est un appareil electro-mécanique de chiffrement utilisée durant la seconde guerre mondiale par le régime nazi. Elle a permis aux militaires allemands de maintenir une commnunication secrète durant une majeure partie de la guerre. Très peu de machine ont survécu du au fait que la majorité des machines ont été détruites par les Alliés à la fin de la guerre.

Il existe plusieurs types de machine, toute utilisée à différentes périodes de la guerre. Dans ce document nous nous intéressons uniquement à la machine Enigma `I`, également connue sous le nom *Ch.11a* par son constructeur CryptoMuseum (2016).

Le chiffrement d'un caractère s'effectue lors de la pression d'une entrée sur le clavier de la machine. Celle-ci met en évidence la sortie *i.e.* un caractère, chiffré sur un voyant lumineux.

La machine Enigma `I` met à disposition plusieurs composants mécaniques paramètrables. Il en existe de trois type: les rotors, les reflecteurs et le plugboard. La figure 1 montre la machine ouverte, et met en évidence les différentes zones des composants.

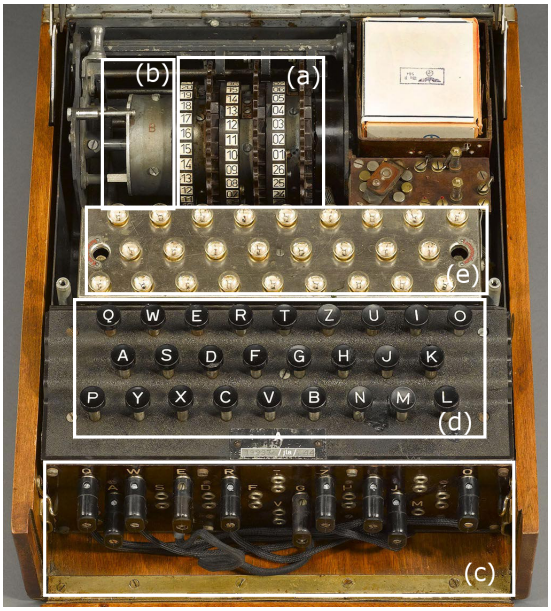

Figure 1: Machine Enigma `I`

	ABCDEFGHIJKLMNOPQRSTUVWXYZ
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ
II	AJDKSIRUXBLHWTMCQGZNPYFVOE
III	BDFHJLCPRTXVZNYEIWGAKMUSQO
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB
V	VZBRGITYUPSDNHLXAWMJQOFECK

Table 1: *Wiring table* des rotors

Rotors

Les rotors sont des composants mécaniques rotatifs. La machine est composée de trois roues adjacentes lors de son fonctionnement. Le modèle Enigma `I` met à disposition cinq rotors numérotés: `I`, `II`, `III`, `IV` et `V`. Les trois rotors doivent être placés sur la zone (a) du schéma. Il existe donc 60 combinaisons de placement possibles.

Pour chaque rotor, il est nécessaire de parametrer: la position de départ et la position d'un anneau. L'anneau est un élément qui permet d'effectuer un décalage dans le chiffrement qu'effectue le rotor. Il existe 26 positions de départ et 26 positions d'anneau. Nous avons donc 26^3 combinaisons possible pour les départs et 26^3 pour les anneaux.

	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	YRUHQSLDPXNGOKMIEBFZCWVJAT
C	FVPJIAOYEDRZXWGCTKUQSBNMHL

Table 2: *Wiring table* des reflecteurs

La fonction du rotor est de remplacer un caractère par un autre. Le tableau 1 indique les caractères de remplacement pour chaque rotor.

Les rotors offrent donc C_{ro} possibilités de configuration, avec:

$$C_{ro} = 60 * 26^3 * 26^3$$

Reflecteurs

Les reflecteurs sont des composants identiques aux rotors, à la différence que dans ce modèle de la machine, ils n'effectuent aucune rotation. Le fonctionnement de la machine nécéssite la mise en place d'un reflecteur. Deux reflecteurs sont mis à disposition nommés: `B` et `C`.

Le reflecteur doit être placé dans la zone (b) du schéma. Dans la version que nous utilisons pour le simulateur seuls les reflecteurs B et C sont utilisés, soit C_{re} choix possibles, avec:

$$C_{re} = 2$$

L'objectif d'un reflecteur est de remplacer un caractère par un autre. Le tableau 2 indique les caractères de remplacement pour chaque reflecteur.

Plugboard

Le dernier élément paramètrable de la machine est un plugboard. La machine est composée d'un seul plugboard, dans lequel sont connécté en paire des caractères alphabétiques. Généralement dix cables sont mis à disposition. Le plugboard permute les caractères entrés avant de les envoyer dans le circuit. Par exemple si les caractères A et B font une paire du plugboard, si le caractère A est entré, c'est le caractère B qui est envoyé dans le reste du circuit et vice-versa. L'ordre d'une paire n'a donc pas d'importance.

Le plugboard offre C_p possibilités de configuration, avec:

$$C_p = 26!/(6! * 10! * 2^{10})$$

Clé de chiffrement d'Enigma

Au total le nombre de possibilté qu'offre Enigma `I` est C_{total}, avec:

$$C_{total} = C_{ro} * C_{re} * C_p \approx 2^{82}$$

Enigma utilise un chiffrement symétrique avec comme clé les différentes combinaisons des composants. La taille de clé que propose Enigma `I` est d'environ 82 bits.

Etat de l'art

Il existe de multiples simulateurs graphiques. Plusieurs d'entre-eux sont disponibles via une application web et d'autres en logiciel bureau. Dans les sections suivantes, plusieurs simulateurs vous sont présentés, en plus des différences notables entre ceux-ci et celui développé.

Universal Enigma

Le simulateur graphique Palloks (2016) est une application web simulant différents modèles d'Enigma. Son interface est de type utilitaire *i.e.* les caractères à chiffrer doivent être entrés dans une zone de texte, et les caratères de sortie sont déployés dans une autre zone de texte. Les choix et configurations des différents composants de la machine s'effectuent via des listes et des boutons. Le chiffrement est automatique et ne nécessite aucune action de l'utilisateur hormis la saisie du texte à chiffrer.

Les similitudes notables entre cette implémentation et celle proposée sont la technologie utilisée *i.e.* le `JavaScript` ainsi qu'une interface utilitaire simple. Ce simulateur propose également une simulation d'une dizaine de modèle de la machine Enigma.

Enigma Simulator de Rijmenants

Le simulateur Rijmenants (2016) est un simulateur de plusieurs modèles d'Enigma, dont le modèle Enigma `I`. Disponible uniquement sous Windows, c'est un des simulateurs graphiques les plus complet, permettant de configurer les composants de la manière des plus réalistes. Le developpeur propose un manuel d'utilisation pour pouvoir utiliser toutes les simulations proposées. Une fonctionnalité du logiciel est de pouvoir écrire un texte à chiffrer. Cependant cette implémentation se révèle être très peu intuitive.

Les similitudes notables entre cette implémentation et celle proposée sont l'interface graphique de la machine. Ce simulateur se révèle être plus complet dans la configuration et la modélisation des composants.

Enigmaco

Le simulateur Enigmaco (2016) est une application web simulant une machine Enigma qui pourrait correspondre au modèle `M3` ou `M4`. Le but principal de ce simulateur est de

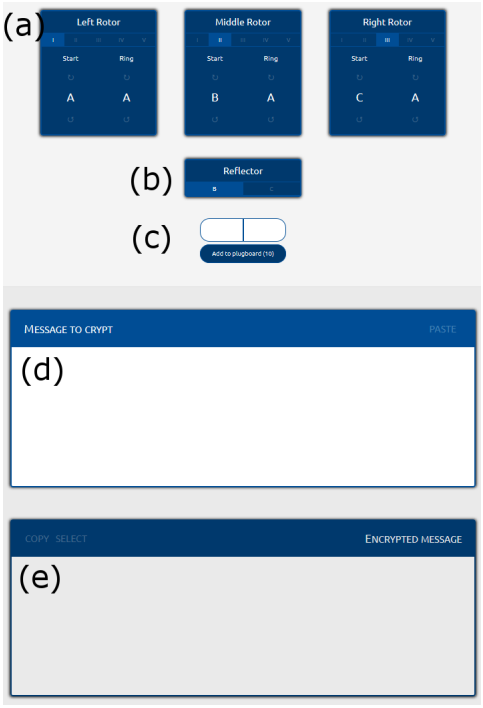

Figure 2: Partie utilitaire du simulateur

montrer le fonctionnement de la machine en illustrant le parcours de chiffrement depuis l'entrée du caractère à chiffrer jusqu'au caractère de sortie chiffré. A chaque chiffrement les rotations ainsi que le circuit parcouru est montré. Il est possible uniquement de configurer les rotors et le plugboard.

Le simulateur proposé

Technologie

Le simulateur graphique que présente ce document a été développé avec les technologies web `JavaScript` pour la logique du programme et les technologies `HTML5` et `CSS3` pour la partie graphique du programme.

Utilitaire

Le simulateur propose une interface de type utilitaire, qui facilite la configuarion des composants de la machine, ainsi qu'un meilleur moyen de saisie du texte à chiffrer. La particularité de cette interface est qu'il est possible d'entrer tout type de caractère pour que lors du déchiffrement du message, les caractères de ponctuation puissent être conservés.La partie utilitaire du simulateur est visible sur la figure 2.

La zone (a) représente les rotors utilisés par la machine pour le chiffrement. Pour chaque coté de la machine *i.e.* gauche, milieu et droit il vous est possible de choisir le rotor désiré. Si un rotor est déjà utilisé dans un autre emplacement, ce dernier change automatiquement de rotor. Dans le cadre d'un emplacement il est possible de changer la position de départ du rotor choisi ainsi que son anneau.

La zone (b) de la figure représente le choix du reflecteur. Deux bouttons `B` et `C` sont cliquable et c'est celui en surbrillance qui est utilisé pour le chiffrement.

La zone (c) permet d'ajouter des paires dans le plugboard. Deux entrées textes dans lesquelles les caractères alphabétiques des paires doivent être entrés. Dans le cas où les caractères ne sont pas alphabétiques ou que les caractères sont déjà utilisés, aucunes paires n'est ajoutés et il vous est nécessaire de remplacer les caractères pour ajouter une nouvelle entrée dans le plugboard. Si vous avez ajouté 10 paires, il ne vous sera plus possible d'en rajouter d'autre. Il est possible de supprimer une paire en cliquant dessus.

La zone (d) est une zone de texte où il est possible d'écrire le texte que la machine doit chiffrer. Tous les caractères sont admissibles mais seuls les caractères alphabétiques seront chiffrés. Les majuscules et les minuscules sont conservées dans la zone de chiffrement. Les autres caractères ne seront pas chiffrés mais sont tout de même retranscrit dans la zone de chiffrement. Il est possible de supprimer du texte. Dans ce cas la machine effectue un retour arrière dans les rotations ce qui permet de garder une cohésion avec le texte chiffré.

La zone (e) est la zone de chiffrement. Les caractères que la machine a chiffrés sont retranscrit dans cette zone de texte. Aucune interaction n'est possible dans cet élément du simulateur, hormis la selection du texte.

Graphique

La partie graphique du simulateur a pour but de simuler la conception de la machine. Comme pour la vrai machine il est possible de l'ouvrir pour configurer certains composants. La figure 3 représente la machine dans son état fermé. La figure 4 représente la machine dans sont état ouvert. Pour ouvrir ou fermer la machine il est nécessaire d'appuyer sur le bouton (e) de la figure 3.

Configuration des rotors

Rotors Pour changer la position des rotors il est nécessaire de cliquer sur la partie supérieure ou inférieure de l'élement rotatif du rotor, dans la partie (a) de la figure 3. Il est possible de changer la position quand la machine est ouverte ou fermée. Pour changer de rotor il est nécessaire d'ouvrir la machine, et de passer le curseur sur le numéro du rotor. Un menu déroulant apparait, la zone (b) de la figure 4, listant tous les rotors de la machine. Il suffit de cliquer sur le numéro du rotor que vous désirez mettre à l'emplacement associé.

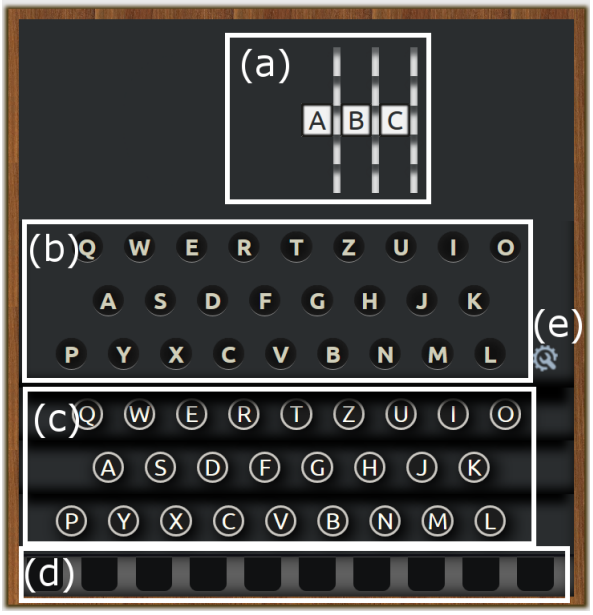

Figure 3: Partie graphique : machine fermée

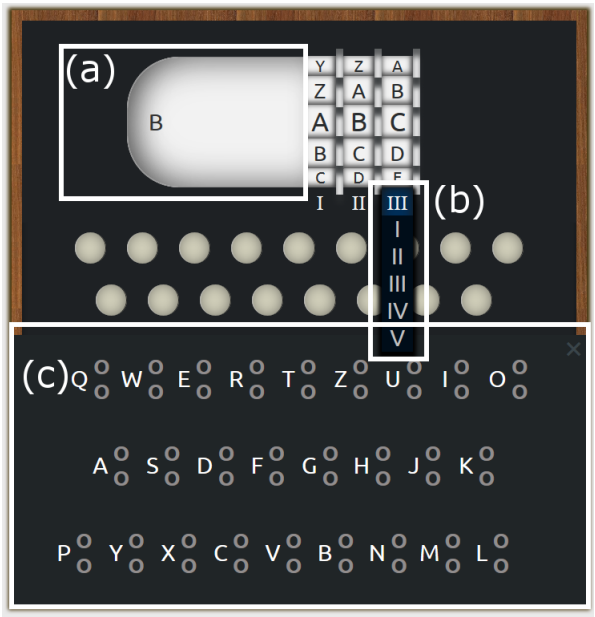

Figure 4: Partie graphique : machine ouverte

Reflector Pour changer le reflector il vous faut ouvrir la machine et cliquer sur la zone (a) de la figure 4, ce qui changera le reflecteur.

Plugboard La zone (c) de la figure 4 est le panneau de configuration du plugboard. Ce panneau est ouvert lors du clique sur la zone (d) de la figure 3. Le panneau peut être affiché peu importe l'état de la machine (ouvert ou fermé). La zone (c) de la figure 4 vous permet d'ajouter des paires dans le plugboard. Pour effectuer cette action, il faut maintenir le clique sur une entrée, et relacher le clique sur une autre entrée. Pour supprimer une paire, il faut effectuer un clique droit sur l'une des entrée.

Entrée/Sortie Pour chiffrer un caractère il faut cliquer sur un caractère du clavier de la zone (c) de la figure 3. Cette action illumine le résultat du chiffrement sur le panneau de la zone (b) de cette même figure.

Conclusion

Dans ce document nous avons brièvement introduit les algorithmes de chiffrement symétrique ainsi que leur fonctionnement. Ensuite nous avons effectué une déscription de la machine Enigma `I` et de ses composants ce qui nous a permis d'effectuer un parallèle avec le chiffrement symètrique et leur implémentation. Ensuite nous avons donné une déscription des différents simulateurs de la machine Enigma disponible sur Internet et des principales fonctionnalités de ceux-ci. Pour finir, nous avons présenté le simulateur que nous proposons, ainsi que son fonctionnement.

Le but du simulateur est de proposer à tous un accés à la machine Enigma, avec pour but de comprendre et d'utiliser les outils de chiffrement qui étaient utilisés dans le passé. Seulement il existe des dizaines de modèle de la machine Enigma, et le simulateur n'implémente qu'un seul de ceux-ci. Il serait intéressant de développer ce simulateur pour d'autres modèles, ce qui permettrait de visualiser aux mieux le développement de cette machine durant le 20ème siècle.

Un autre aspect qui pourrait être améliorer est la visualisation physique de la machine. Une fonctionnalité intéressante serait de pouvoir visualiser en 3D la machine complète ainsi que chaque composant. Entre autre un aspect plus pédagogique serait de pouvoir visualiser le circuit de chiffrement d'un caractère *i.e.* composant par composant.

References

Boulahya, H. (2016). http://student.ulb.ac.be/hboulahy/enigma/.

CryptoMuseum (2016). http://cryptomuseum.com/crypto/enigma/i/index.htm.

Enigmaco (2016). http://enigmaco.de/enigma.

Palloks, D. (2009-2016). https://people.physik.hu-berlin.de/p̄alloks/js/enigma/enigma-u_v20_en.html.

Priyadarshini Patil, P. N. (11-12 December 2015). A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish. *Procedia Computer Science 78 (2016) 617 – 624*.

Rijmenants, D. (2004-2016). http://users.telenet.be/d.rijmenants.

The McGraw-Hill Companies, I. (2016). Cryptography. *McGraw-Hill Concise Encyclopedia of Engineering*, page //encyclopedia2.thefreedictionary.com/cryptography.