

2014-2015

Projet Enigma

Compte-Rendu

DUT Informatique (S4)

TROUVE Robin
KISSI Naïm
DE LIMA Marianna

Encadré par:

M. ROY

Sommaire

Introduction	2
1. Enigma : Machine de cryptage	3
1.1. Création d'Enigma	3
1.1.1. Remise en contexte	3
1.1.2. Utilisation d'Enigma	4
1.2. Fonctionnement d'Enigma	5
1.2.1. Les rotors	5
1.2.2. Le plugboard.....	6
1.2.3. Le réflecteur.....	7
1.3. Cryptanalyse par Turing	9
2. Enigma : Simulation informatique	10
2.1. Organisation du projet	10
2.1.1. Choix et contraintes	10
2.1.2. Outils de travail	12
2.1.3. Gestion de l'équipe	12
2.2. Représentation d'Enigma	15
2.2.1. Conception UML	15
2.2.2. Logique de fonctionnement	
2.3. Difficultés rencontrées et solutions retenues	
3. Manuel utilisateur	
Bilan	
Annexes	

Introduction

Dans le cadre de notre DUT Informatique, en semestre 4, nous sommes amenés à réaliser un projet alliant mathématiques et informatique afin d'appliquer nos connaissances et la méthodologie que nous avons pu acquérir au cours de notre formation.

Le sujet de ce projet est la machine Enigma, machine de cryptage la plus connue et utilisée lors de la Seconde Guerre Mondiale. Il s'agit donc ici de comprendre son fonctionnement, ses mécanismes et de pouvoir reproduire son comportement de manière informatisée.

Ce compte-rendu détaille notre démarche pour aborder le sujet, le comprendre et enfin réaliser techniquement le projet en s'organisant au sein du trinôme, en utilisant des outils et les méthodes appris en cours.

Nous allons donc voir dans une première partie ce qu'est la machine Enigma, son rôle, son fonctionnement et nous nous intéresserons aussi à sa cryptanalyse par Alan Turing pour comprendre ses failles. Nous verrons ensuite comment nous nous sommes organisés pour mener le projet à bien en mettant toutes nos connaissances en œuvre et nous verrons aussi les difficultés nous avons rencontrés et comment nous les avons surmontées.

1. Enigma : Machine de cryptage

1.1. Création d'Enigma

1.1.1. Remise en contexte

Enigma est une machine électromécanique permettant de crypter et de décrypter un message. Cette machine est essentiellement composée de trois rotors, d'un réflecteur, d'un plugboard, d'un clavier et d'un afficheur de lettre cryptée mais nous détailleront plus en profondeur tous ces composants dans la partie suivante et nous expliqueront les fonctionnalités de chacun.



Arthur Scherbius

Enigma a été créée par un ingénieur en électricité allemand du nom d'Arthur Scherbius, né en 1878, qui a étudié à Munich puis à Hanovre.

Initialement il n'avait pas pour ambition de créer une machine de chiffrement d'ailleurs à la fin de ses études en 1903 il consacre sa thèse à des systèmes de turbines à eau.

C'est dans les années 1910 plus précisément à partir de 1918 qu'Arthur Scherbius commence à s'intéresser aux systèmes de chiffrement, il décide alors d'entamer la création d'un système de cryptage révolutionnaire pour l'époque du nom d'Enigma.

Enigma était le seul système de cryptage possédant des rotors désynchronisés et un plugboard, permettant de décupler le nombre de combinaison possible et de dépasser de loin tous les systèmes de chiffrement de l'époque en terme de sécurité (ex : le chiffre de Vigenère).

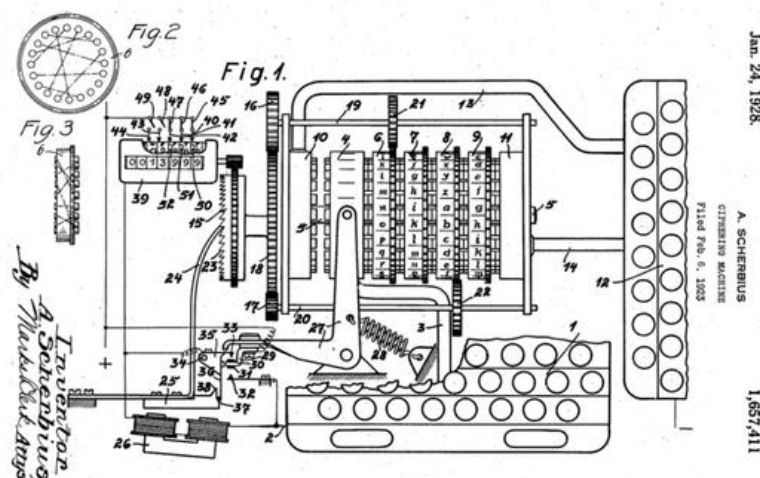
Créé par Vigenère lui-même en 1586, la méthode du chiffre de Vigenère consistait à substituer une lettre par une autre avec un chiffrement polyalphabétique (il utilisait 10 alphabets différents). Cette méthode de chiffrement a résisté trois siècles aux cryptanalystes et était donc une des méthodes de chiffrement les plus sûres. Cependant un major prussien du nom de Friedrich Kasiski a réussi à briser le mystère de ce système en 1863, le rendant ainsi obsolète.



Vigenère

La machine Enigma, de par son fonctionnement offrant un grand nombre de possibilités de combinaison, fut une véritable révolution à l'époque, elle était considérée comme inviolable car il fallait avoir la même machine que celle qui a crypté le message pour avoir une chance de le décrypter. De plus, il était impossible de tester toutes les possibilités de combinaison d'Enigma sans connaître la combinaison initiale des rotors.

Afin de protéger sa création, Arthur Scherbius a décidé de breveter son œuvre, et d'autres talentueux inventeurs Koch firent de même comme le hollandais en déposant un brevet en 1919. Ce dernier fut racheté par la société de Scherbius afin d'éviter que cela ne leur porte préjudice dans le futur.



Brevet déposé par
Arthur Scherbius

1.1.2. Utilisation d'Enigma



Enigma-A

Après avoir breveté son invention, Arthur Scherbius décida de commercialiser sa machine l'Enigma-A or son invention n'eut pas le succès escompté. En effet c'est un échec commercial car sa machine est considérée comme « trop chère » avoisinant les 30 000 euros, pourtant plus tard trois autres versions commerciales verront le jour.

Ici nous n'allons pas nous intéresser à la version commercial mais plutôt à la version militaire qui a été surnommée l'Enigma-D et qui a été adoptée par l'armée allemande dès 1926 plus précisément par la Marine puis par l'armée de terre en 1929. Par la suite, la machine a été exploitée par les nazis qui l'ont renommée « machine M ».



Enigma-D

Enigma fut l'un des plus grands atouts de communication et était très utilisée par l'Allemagne nazie et ses alliés pendant la seconde guerre mondiale. Ils l'utilisaient pour les bulletins météo mais surtout pour les informations sensibles notamment sur les tactiques militaires et les stratégies à adopter face à l'ennemi. Les nazis avaient donc une totale confiance dans le système d'Arthur Scherbius. Ils changeaient tout de même régulièrement la configuration des rotors pour plus de sécurité et notaient sur un livre les positions du jour de chaque rotor (cf annexes).

Les messages étaient cryptés par la machine Enigma avec les positions du jour et au début du message crypté, la clé était incluse pour permettre au receveur de trouver la bonne position afin de décrypter le message. Evidemment les deux machines devaient être les mêmes pour avoir un réglage de machine cohérent entre le cryptage et le décryptage. Le message crypté était envoyé un morse par onde radio au destinataire.

—	A	—	S
—	B	—	T
—	C	—	U
—	D	—	V
—	E	—	W
—	F	—	X
—	G	—	Y
—	H	—	Z
—	I	—	1
—	J	—	2
—	K	—	3
—	L	—	4
—	M	—	5
—	N	—	6
—	O	—	7
—	P	—	8
—	Q	—	9
—	R	—	0

Le morse est un langage qui permet de communiquer à distance via onde radio, ce langage est composé de tiret et de point et est accompagné d'un dictionnaire permettant de traduire les tirets et les points en lettre. On utilise ce langage par le biais d'un télégraphe Morse, cet outil se compose essentiellement d'un manipulateur, d'un relais et d'un récepteur.

Le manipulateur est composé d'un socle de bois qui possède deux bornes et un levier, qui peut osciller verticalement.

Pour envoyer un message, il faut appuyer sur la poignée du levier pour que le courant puisse passer, puis dès que l'on relâche le levier le courant s'interrompt.

C'est de cette manière que la manipulation est transmise au récepteur via onde radio c'est à dire entre 9 kHz à 3 000 GHz.

Le récepteur utilise un électro-aimant qui est connecté à la Terre et au fil de ligne.

Dès que le courant passe dans le récepteur la plaque de fer de l'électro-aimant est attirée et repoussée grâce au ressort de rappel due au passage ou à l'interruption du courant.

Grâce à ce mécanisme le levier pouvait ainsi osciller de haut en bas, en bas dès que le courant passé dans le récepteur et donc le levier munie d'une pointe pouvait laisser des traces sur le papier et le levier était en position haut des que le courant était interrompue ainsi le résultat était récupéré sur le papier et pouvait être traduit en lettre via le dictionnaire Morse.

Le relais quant à lui été uniquement utilisé pour augmenter la puissance du courant électrique, en effet le courant de ligne à lui seul n'était pas suffisant pour laisser des traces sur le papier du coup le relais lui, est composé d'une pile et il pouvait ainsi ajouter son courant à celui du courant de ligne pour amplifier le courant total.

1.2. Fonctionnement d'Enigma

1.2.1. Les rotors

Nous allons à présent voir en détail comment Enigma fonctionne, quelles sont ses particularités qui l'ont rendu si difficile à « casser ».

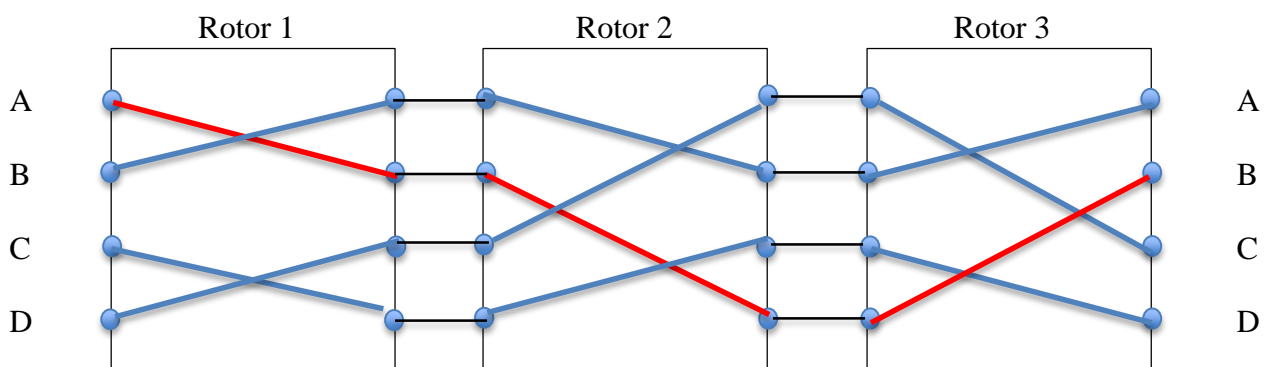
La puissance d'Enigma réside dans le fait qu'elle est imprévisible en terme de chiffrement des mots rentrés et cela est directement permis par sa structure interne. C'est la combinaison de ses composants qui la rend si performante mais quels sont-ils ? En tant que machine électromécanique, Enigma est composée de rotors fonctionnant avec des contacts électriques permettant la substitution poly-alphabétique, c'est d'ailleurs une de ses particularités.



Les rotors servent de connexion électriques, ils sont au nombre de 3 dans la machine et pouvaient être choisis parmi 5 rotors en tout. Leur particularité vient du fait qu'ils sont cylindriques et fixés sur un axe autour duquel ils peuvent tourner. A chaque lettre tapée, le rotor effectue une rotation qui change complètement la donne pour la lettre suivante car du coup, la permutation sera différente pour chaque lettre même si celle-ci est retapée.

C'est un des points forts d'Enigma car de ce fait, l'analyse par fréquence qui consiste à repérer les lettres qui reviennent fréquemment dans un message crypté est impossible. Mais comme signalé, il y a 3 rotors en tout. Chaque rotor représente les lettres/chiffres que l'on veut crypter. Par exemple, si on prend l'alphabet de 26 lettres, chaque rotor aura 26 positions. Le 1^{er} rotor tourne d'un cran à chaque fois qu'une lettre est tapée, de sa 26^e position à sa position initiale, il déclenche le 2^e rotor qui lui aussi tourne d'un cran. Lorsque le 2^e rotor effectue sa rotation de sa 26^e lettre à sa position initiale, il déclenche à son tour le 3^e rotor. Les rotors reviennent à leur position initiale lorsqu'ils ont tous parcouru leur 26 positions. Chaque rotor pouvait être positionné de 1 à 26 avant de commencer à taper le message.

Nous avons schématisé les 3 rotors avec 4 lettres selon un circuit électrique de cette manière :



On peut voir ici que si on tape lettre « A », elle sera permutée en « B » à l'issue du rotor 1 puis en « D » et enfin en « B ». Le rotor 1 tournera d'un cran et ses sorties seront décalées ce qui permettra d'avoir une lettre cryptée différente même si on retape à nouveau « A ».

Si on calcule le nombre de possibilités de cryptage qu'offrent les rotors, nous avons :

$$5 * 4 * 3 = 60$$

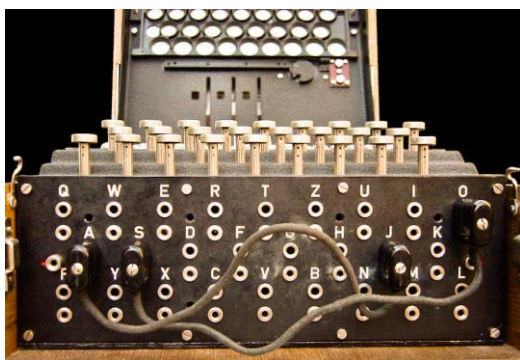
$$26^3 = 17\,576$$

$$\text{Soit : } 60 * 17\,576 = 1\,054\,560$$

Jusqu'ici nous avons donc 60 possibilités de choix de rotors (3 parmi 5) et 17 576 (pour un alphabet de 26 lettres) positions possibles des rotors car chaque rotor à 26 positions donc $26 \times 26 \times 26$ soit un total de 17 576 possibilités de cryptage. Si l'alphabet comporte plus de caractères, cela augmentera le nombre de positions possibles des rotors et donc le nombre de possibilités total.

1.2.2. Le plugboard

Mais Enigma ne s'arrête pas à ces trois rotors tournant, en effet, un des composants central de cette machine est le tableau de connexion (plugboard), situé devant la machine et permettant d'effectuer 10 paires de permutation. Le plugboard était spécialement conçu pour les machines utilisées à des fins militaires, les versions commerciales en étaient dépourvues.



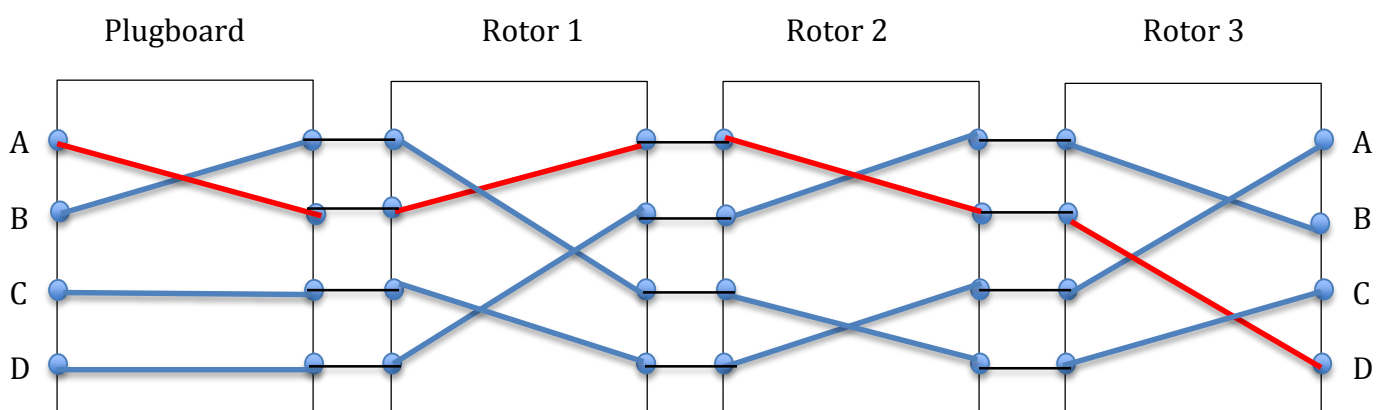
Les permutations sont commutatives c'est-à-dire que si la lettre « A » est reliée à la lettre « B » alors la lettre « A » sera permutée avec la lettre « B » mais la lettre « B » sera permutée avec la lettre « A ».

Il y a donc 20 lettres permutées et 6 inchangées dans un alphabet de 26 lettres.

Le but du plugboard était de brouiller les pistes car une lettre tapée était d'abord permutée suivant le tableau de connexion puis codée.

Concrètement, cela signifie que si « A » était permutée avec « B », c'est la lettre « B » qui serait effectivement cryptée en passant dans les rotors.

Nous avons donc enrichi notre schéma (cf rotors ci-dessus) avec le plugboard ce qui nous donne sur un alphabet de 4 lettres :



Dans ce cas-ci, les lettres « A » et « B » sont permutées alors que les lettres « C » et « D » restent inchangées. Si on veut crypter la lettre « A », c'est donc en fait la lettre « B » qui va être cryptée et on obtiendra donc en permutations successives: A→B, B→A, A→B, B→D.

Si nous calculons les possibilités qu'offrent les branchements frontaux pour un alphabet de 26 lettres nous avons :

$$\frac{26!}{6!10!2^{10}} = 150\,738\,274\,937\,250$$

En effet, nous avons 26 combinaisons de lettres (26x25x24...x1) ce qui justifie le « 26 ! ». Cependant, nous ne voulons faire que 10 paires de lettres donc 6 lettres restent non permutées. Etant donné que l'ordre des combinaisons n'importe pas, nous pouvons diviser par « 6 ! » et multiplier par le nombre de combinaison possible pour les 10 paires soit « 10 ! ». Enfin les paires sont constituées de deux lettres interchangeables, on peut alors diviser par « 2 » et comme il y a 10 paires de lettres cela nous donne « 2¹⁰ »

Le plugboard est donc un élément central car c'est lui qui augmente considérablement le nombre de possibilités.

Si on rajoute les possibilités qu'offraient les rotors nous avons :

$$150\,738\,274\,937\,250 * 1\,054\,560 = 158\,962\,555\,217\,826\,360\,000$$

Voilà donc le nombre de possibilités de cryptage que permettait Enigma grâce à la combinaison de ses composants.

1.2.3. Le réflecteur

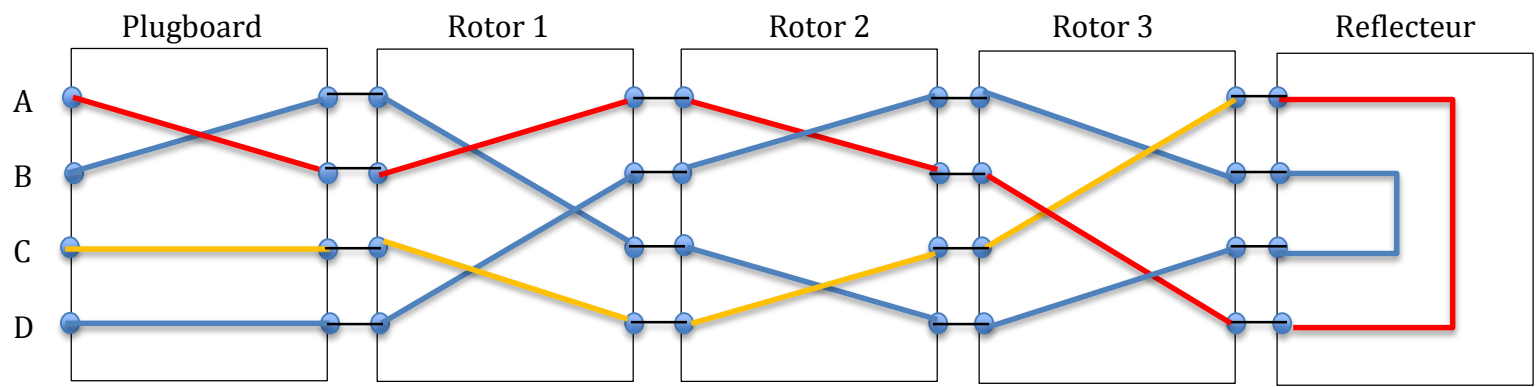
Cependant, à ce stade, la machine est capable de crypter mais pas de décrypter. Il faudrait donc une machine pour crypter et créer une seconde machine pour décrypter. Pour pallier à ce problème, Enigma s'est dotée d'un réflecteur, une sorte de rotor fixe qui a pour but de faire une ultime permutation et de renvoyer le courant dans l'autre sens. De ce fait, il inverse par paires les lettres et permet de lier les lettres de façon à pouvoir rendre le cryptage réversible. Concrètement, si on tape la lettre « A » et qu'elle est cryptée en « D » alors lorsqu'on décryptera la lettre « D » elle renverra « A » (la machine doit avoir les mêmes paramétrages pour le cryptage et le décryptage).



Il existait plusieurs versions de réflecteur. La version B était la plus couramment utilisée mais il a aussi existé les versions C et D. Certaines de ces versions permettant de positionner le réflecteur de différentes manières (différentes positions un peu comme les rotors).

Le principe même du réflecteur empêchait toute lettre d'être codée par elle-même ce qui sera largement exploité lors de la cryptanalyse de Turing que nous verrons dans la prochaine partie.

Nous pouvons enrichir une dernière fois notre schéma pour montrer une version complète du fonctionnement d'Enigma :



Légende : Cryptage : chemin aller ——— (red)
 chemin retour ——— (yellow)
 Decryptage : chemin aller ——— (yellow)
 chemin retour ——— (red)

Reprenons notre exemple pour crypter la lettre « A ».

ALLER	REFLECTEUR	RETOUR
Plugboard : « A » devient « B »	Réfecteur : « D » devient « A »	Rotor 3 : « A » devient « C »
Rotor 1 : « B » devient « A »		Rotor 2 : « C » devient « D »
Rotor 2 : « A » devient « B »		Rotor 1 : « D » devient « C »
Rotor 3 : « B » devient « D »		Plugboard : « C » reste « C »

« A » est donc cryptée en « C » et si on veut décrypter « C », on remonte le chemin retour jusqu'au début du chemin aller et on obtient bien « A ». Lorsque la lettre est passée par tous les composants, une pile électrique, alimentant Enigma, permet d'allumer la lampe correspond à la lettre cryptée/décryptée que l'on doit alors noter.

Le fonctionnement d'Enigma permet donc de faire une machine à crypter et décrypter très puissante, avec très peu de failles. Cependant, la seule faiblesse apparente qu'elle a (une lettre ne peut être cryptée par elle-même) va être le point de départ de la cryptanalyse d'Alan Turing.

1.3. Cryptanalyse par Alan Turing

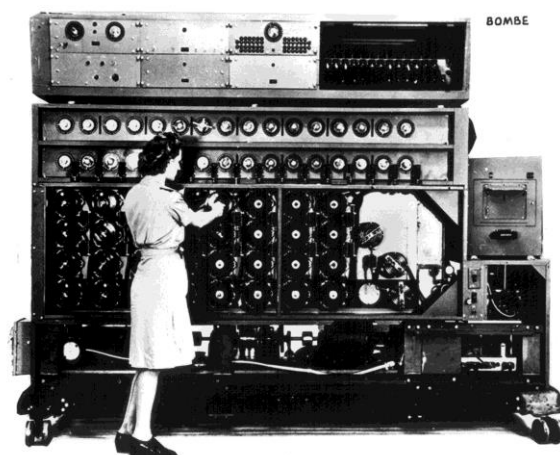


Les nazis considéraient le système de chiffrement d'Enigma inviolable mais un homme a réussi l'exploit, déchiffrer Enigma, cet homme c'est Alan Mathison Turing dit Alan Turing qui était mathématicien, cryptologue et informaticien britannique, il est né le 23 juin 1912 et mort le 7 juin 1954.

Alan Turing crée une machine surnommée « Bomb » qui permet de tester des combinaisons possible d'Enigma mais pas toutes car cela serait impossible dans des délais humain.

Il réduit donc les combinaisons à tester grâce à la méthode qu'il a trouvé. Il se sert d'une faille du système Enigma, en effet une lettre à cryptée n'est jamais substituée à elle-même du fait du réflecteur donc un N ne pourra jamais donner un N.

De plus, l'autre faille venait du système allemand en lui-même, c'est à dire qu'ils avaient l'habitude d'envoyer un bulletin météo tous les jours à 6h et ce bulletin météo avait toujours la même forme. Il contenait notamment le mot « wetterbericht » qui voulait dire bulletin météo en allemand et se finissait toujours par « Hitler ».



Avec ces informations, Alan Turing comparait les mots clés allemands avec le message codé en vérifiant que chaque lettre du mot clé soit différente du message. Si ce n'était pas le cas il déplaçait le mot clé jusqu'à que toute les lettres soient différentes, cela signifiait alors que le mot clé pouvait peut-être se situer à cet emplacement dans le message codé.

A partir de cela, la machine Bomb testait les positions des rotors en fonction des couples du plugboard. C'est-à-dire qu'on positionnait le Rotor 1 à 1 par exemple et on faisait la supposition que dans le plugboard deux lettres étaient liées. La machine vérifiait que la supposition était exacte en lisant le message codé et le mot-clé. Si on tombait sur une contradiction, par exemple on suppose A-D branchés dans le plugboard et au fil de la lecture on a un autre couple A-Z alors qu'une même lettre ne peut pas être branchée deux fois dans le plugboard, alors la supposition de départ était fausse et la position supposée des rotors aussi et on essayait alors une autre position. Pour accélérer les choses, Turing a émis l'idée que si il y avait une contradiction alors tous les autres couples trouvés qui découlaient de la supposition initiale fausse étaient faux aussi et n'avaient alors pas besoin d'être revérifiés.

Finalement, la machine Bomb était capable de trouver les couples du plugboard et les positions de rotors utilisées pour crypter le message en 20 minutes. Il ne restait alors plus qu'à décrypter le code avec les bons réglages.

Cette phase d'analyse nous a véritablement permis de cerner le sujet et de mieux comprendre le rôle de chaque composant de la machine Enigma. De plus, cela nous a aussi permis d'avoir des pistes notamment pour le décryptage en s'appuyant de la cryptanalyse faite par Alan Turing.

2. Enigma : Simulation informatique

2.1. Organisation du projet

Avant de nous lancer dans le développement du projet, nous avons dû dans un premier temps nous organiser sur différents points.

2.1.1. Choix et contraintes

Nous avons dû effectuer certains choix avant de commencer à développer et même avant de pouvoir conceptualiser le projet.

Nous nous sommes tout d'abord posé la question du choix du langage de programmation. Celui-ci étant complètement libre avec pour seule obligation, avoir une interface graphique, nous pouvions partir sur du développement logiciel (C, C++, Java) mais aussi sur du développement web (html, css, javascript). Parmi les langages que nous connaissons, celui que nous avons le plus utilisé et où nous nous sentons le plus à l'aise reste le langage Java.



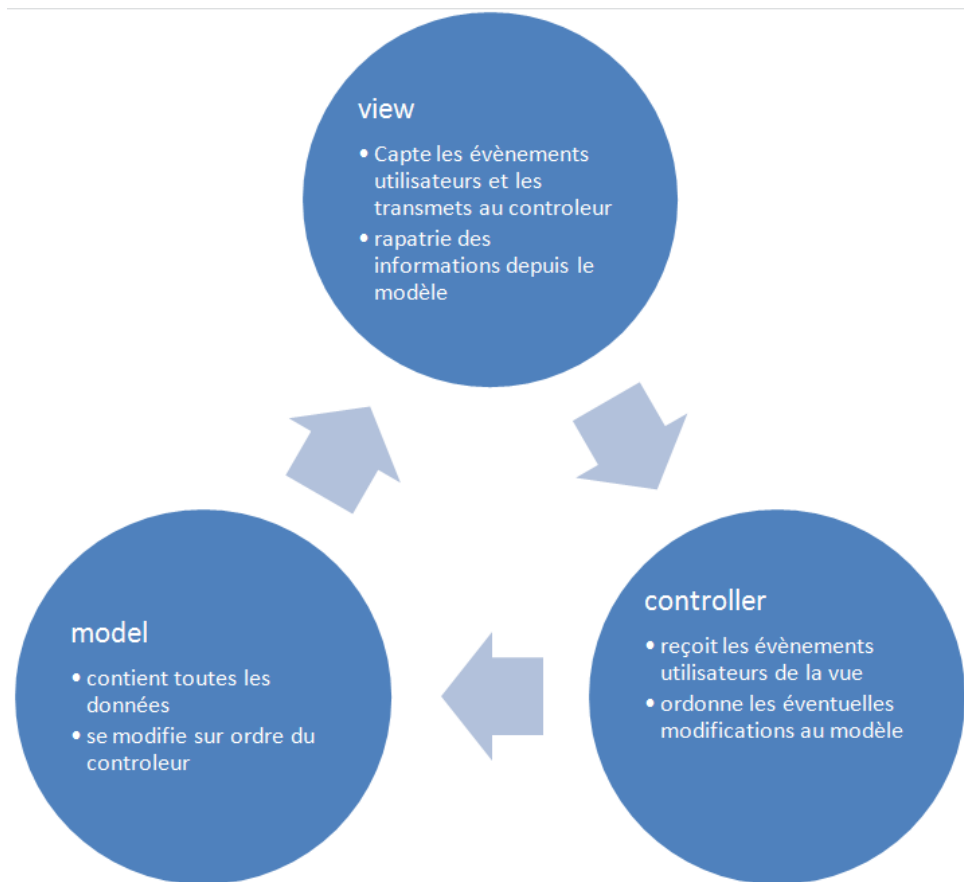
C'est donc le langage de programmation Java, langage orienté objet, que nous avons retenu étant donné que nous avons déjà eu un cours d'interface Homme Machine facilitant le développement de l'interface graphique et que nous sommes à l'aise avec la notion d'objet qui nous a paru cohérent avec les composants de la machine Enigma (nous détaillerons ce point dans une prochaine partie).

Nous avons eu, au semestre dernier, un cours sur les principaux design pattern que l'on peut utiliser afin d'avoir une bonne conception d'un projet permettant de décrire une solution standard à un problème de conception logiciel qui peut être par la suite réutilisé sans avoir à modifier le code existant (dans le cas de rajout de classes par exemples). Les design pattern permettent de respecter un certain nombre de bonnes pratiques permettant une conception optimisée et de ce fait un code clair et organisé.

Dans le cadre de notre projet, nous avons décidé d'utiliser le design pattern MVC (Modèle Vue Contrôleur) permettant de faire communiquer les différentes couches de notre projet de façon événementielle c'est-à-dire qu'une action de l'utilisateur via l'interface graphique (la vue) déclenche automatiquement un événement dans le contrôleur qui lui-même se chargera de notifier la couche modèle (c'est le cœur du projet, elle contient toutes les données principales et se charge des principaux calcul).

Afin de faciliter cette programmation événementielle, nous avons implémenté les classes observer et observable définie par défaut en Java et pour créer l'interface graphique, nous avons utilisé la bibliothèque Swing de Java. Nous avons ainsi défini l'architecture globale de notre projet et commencé la phase de conception.

Voici un petit schéma explicatif du design pattern MVC:



Source : <http://raphael-waeselynck.developpez.com/tutoriels/java/java-me/mvc/>

2.1.2. Outils de travail

Ces choix nous ont permis de définir les outils de travail que nous allons utiliser pour partager notre travail et communiquer efficacement.



Comme appris en cours de méthodologie, nous avons utilisé Github, une plateforme de développement collaboratif basée sur git, un outil de versionning. Cet outil permet de mettre en ligne notre projet et les évolutions apportées de façon à ce que tous les membres de l'équipe aient la dernière version du projet disponible et puisse rendre accessible instantanément toutes les modifications effectuées. Cela facilite grandement la création de projet et nous permet d'être très réactifs quant aux erreurs qui pourraient y avoir sur le projet pour les corriger rapidement et ne pas continuer de développer sur une mauvaise base.

Concernant le développement, nous avons décidé d'utiliser Eclipse du au choix du langage de programmation qui est un IDE (Integrated Development Environment) permettant de développer des logiciel en langage Java et de faciliter les tests fonctionnels. C'est un des IDE les plus utilisé pour le développement Java (avec netbeans) et c'est aussi celui que nous connaissons le mieux car nous l'avons déjà utilisé lors d'un projet ultérieur et lors des séances de programmation à l'IUT.



Nous avons aussi été amenés à utiliser le logiciel Mumble, un logiciel VoIP, afin de communiquer oralement en équipe lorsque nous ne pouvions pas nous voir à l'IUT. Cela nous a permis de communiquer efficacement, de réfléchir aux éventuelles difficultés et de proposer des solutions facilement sans avoir à attendre de se retrouver à l'IUT pour en parler.

Ces outils ont été une aide pour avoir une meilleure gestion de l'équipe mais celle-ci s'est aussi faite autour d'autres points que nous allons détailler.

2.1.3. Gestion de l'équipe

Dans un projet, il est important d'avoir une équipe qui sait communiquer, qui s'investi et il est aussi important de répartir les tâches à chaque membre afin d'optimiser le développement du projet.

Dans un premier temps, il était important de se mettre au point sur les connaissances que nous avons acquises sur la machine Enigma lors de nos recherches afin d'avoir une vue générale et cohérente du projet par tous les membres de l'équipe. Pour ce faire, nous avons organisé des petites réunions où nous avons expliqué à chacun ce que nous avons compris ou ce que nous n'avions pas compris pour que l'on puisse lever les zones d'ombres restantes qui nuisent au développement du projet. Ces réunions ont été l'occasion de schématiser les problèmes et d'apporter des solutions de conception. Les avis sur les différentes possibilités de conception nous ont permis d'enrichir le projet et de réfléchir sur des solutions plus optimisée que ce qui était proposé initialement. Cela nous a permis d'être d'un commun accord sur la façon dont nous allons

procéder pour développer le projet. Ces petites réunions ont été la base d'un travail d'équipe solide et efficace.

Par la suite il a été nécessaire de diviser le projet en plusieurs tâches notamment dû au choix de conception que nous avons fait (architecture MVC) et qui nous a permis de développer indépendamment et parallèlement chaque partie. De ce fait chaque membre de l'équipe s'est occupé d'une des couches de l'architecture 3-tiers c'est-à-dire : la partie métier, la partie interface et la partie contrôleur. Pour combler les dépendances entre ces couches nous avons mis en place un « Mock » qui permet de simuler une classe même si celle-ci n'est pas encore opérationnelle. Plus concrètement, il s'agit d'une classe simplifiée qui garde le squelette de la classe réelle mais qui renverra juste les valeurs attendues sans effectuer de calcul (contrairement à la classe réelle).

De plus, nous avons constitué une maquette de l'interface pour que la personne en charge de la partie Vue puisse suivre un modèle où nous étions mis d'accord. Celle-ci se présente comme ceci :

The screenshot shows a window titled "Enigma" with a standard Windows-style title bar (minimize, maximize, close buttons). The interface is divided into two main sections.

Left Section (Reglages):

- Rotors (positions initiales):** Three input fields labeled "Rotor 1", "Rotor 2", and "Rotor 3".
- Rotors (positions actuelles):** Three input fields labeled "Rotor 1", "Rotor 2", and "Rotor 3".
- Positionner les rotors:** Three input fields labeled "Rotor 1", "Rotor 2", and "Rotor 3".
- Appliquer:** A button at the bottom of the settings section.

Right Section:

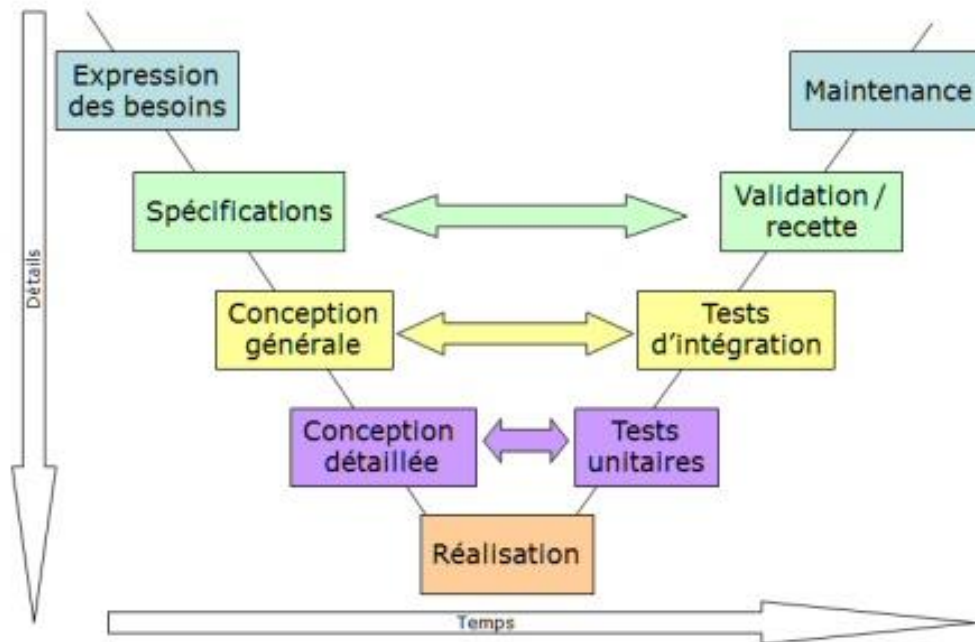
- Clavier revelateur:** A table showing the cipher mapping.

A	B	C	D	E	F	G	0	1	2	3
H	I	J	K	L	M	N	4	5	6	7
O	P	Q	R	S	T	U	8	9		
V	W	X	Y	Z						

 Below the table, it says "Espace" followed by ". , ? !".
- Texte crypte:** A large empty text area for encrypted text.
- Texte en clair:** A large empty text area for decrypted text.
- Parametres inconnus:** A checkbox.
- Decrypter:** A button.

Afin de respecter les délais, et d'avoir un point de repère temporel sur le travail effectué, nous avons conçu un diagramme de Gantt prévisionnel nous permettant de mieux nous situer dans le temps et d'améliorer notre efficacité (voir annexe diagramme.pdf).

Nos méthodes de travail se sont apparentées aux méthodes agiles pour la gestion de projet et plus précisément Scrum du fait de nos réunions, de nos découpage de tâches mais aussi parce que lorsque nous avons terminés une micro-tâche (ex : une fonction complexe d'une classe), nous la testons et nous étions susceptible de modifier pour l'adapter. Plus précisément, nous n'avons pas suivi un cycle en V :



Source : <http://www.methodesagiles.info/Agilite.php>

Nous avons réalisé chaque fonctions puis effectués des tests fonctionnels et corriger/adapter au besoin. Cette méthode à l'avantage d'être moins rigide que le cycle en V et de permettre une évaluation quotidienne des fonctionnalités.

Grâce à cela, la gestion de l'équipe a été grandement facilitée et le travail d'équipe a été plus efficace ainsi que la mise en place du projet.

2.2. Représentation d'Enigma

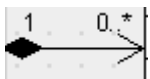
Une part importante dans la simulation d'Enigma a été de modéliser la machine pour mettre en valeur les composants et les fonctionnalités primordiales de la machine.

2.2.1. Conception UML



L'UML (Unified Modeling Language) est un langage de modélisation qui subvient durant la phase d'analyse d'un projet (pour notre cas, juste après l'analyse de la machine Enigma). Il permet d'avoir une vue globale du projet avec une possible manière de fonctionner. La conception UML permet donc de faire le squelette du programme et oblige à se poser les bonnes questions au niveau des fonctionnalités et de la logique de fonctionnement avant de commencer à programmer. Il y a plusieurs types de diagrammes réalisables : diagrammes de cas d'utilisation, diagrammes de séquence, diagramme d'activité... Nous avons choisi d'effectuer uniquement le diagramme de classe qui permettait répondre à nos principales interrogations. Il consiste à représenter les principales classes qui seront présentes dans le programme et leurs lien avec les autres classes.

Nous avons gardé tous les composants de la machine car ils jouaient tous un rôle important dans le fonctionnement d'Enigma. Ainsi, dans notre diagramme UML que nous avons établi après l'étude d'Enigma, nous retrouvons les rotors, le plugboard et le réflecteur. Cette partie est la partie « Métier » et le cœur même du programme. C'est là où les calculs seront effectués, et c'est cette partie qui représente Enigma en soit.

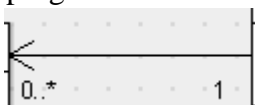


Flèche de composition

Nous pouvons y voir la classe Machine qui peut être vue comme la boîte d'Enigma. A l'intérieur de cette boîte nous avons les rotors, le plugboard et le réflecteur. Notre UML montre qu'Enigma est « composée » de ces éléments. La machine entière est capable de crypter, décrypter grâce à l'interaction de ses composants. C'est la classe Machine qui se chargera de faire le lien entre eux. Par exemple, elle ira chercher la correspondance d'une lettre dans le plugboard puis la transmettra aux rotors puis au réflecteur et indiquera le chemin inverse.

Les classes Rotor, Réflecteur, et Plugboard ne sont autre qu'une reproduction de ce que nous avons compris sur leur fonctionnement : les rotors lient deux lettres ensembles et tournent, le plugboard fait 10 couples de lettres et le réflecteur effectue une ultime permutation.

Nous avons ensuite la classe Vue qui concerne tout ce qui est visuel et saisie utilisateur: champ de texte, affichage des messages cryptés et décryptés. C'est une interface qui fait le lien entre l'utilisateur et le programme.



Flèche d'association

La classe Vue récupère automatiquement les modifications qui s'effectuent via la classe Machine et se met à jour. Pour se faire, la classe Vue est donc « associée » à la classe Machine.

La classe Vue et la classe Machine sont finalement associées à la classe Controleur qui permet d'harmoniser le tout. La classe Controleur est déclenchée à chaque action de l'utilisateur, elle vérifie les informations saisies avant de les envoyer à la classe Machine. Cela permet d'éviter tout plantage du programme à cause d'informations qui ne seraient pas attendues. Elle peut aussi mettre à jour la Vue (affichage d'un message d'erreur par exemple).

Même si le diagramme de classe a constitué la base de notre code, nous avons dû effectuer quelques modifications au cours du projet afin de s'adapter à de nouveaux besoins apparus en programmant. Sans conception, ces modifications auraient été bien plus nombreuses et le risque d'un mauvais fonctionnement entre toutes les classes aurait été plus élevé.

2.2.2. Logique de fonctionnement

- Entrées/sorties des rotors (vu comme un circuit) représenté par un tableau
- Cryptage caractère par caractère (listener de l'interface)
- Décryptage par chaîne de caractère (non implémenté)
- Dictionnaire de mot (non implémenté)
- Création des circuits différents pour chaque rotors

2.3. Difficultés rencontrées et solutions retenues

- Complexité algorithmique : parcours de tableaux $O(n)$ choix : tableaux miroirs
- Décryptage de chaîne : Etude des mots courants à placer
-

Bilan

Nous avons trouvé ce projet très intéressant car même si nous connaissions la machine Enigma, nous ne savions pas concrètement comment elle fonctionnait. Cela nous a alors permis d'acquérir des notions de cryptographie supplémentaires car lors de nos recherches, nous avons aussi comparé le fonctionnement d'Enigma avec d'autres méthodes de cryptage et décryptage et nous nous sommes intéressés à la cryptanalyse en générale.

Sur le plan informatique, nous avons essayé de mettre en pratique toutes les connaissances que nous avons pu acquérir jusque-là dans notre formation et notamment pour la gestion de projet. Se faisant, nous avons eu un aperçu réaliste des phases d'analyse et de conception que nous devons dorénavant appliquer dans chaque projet car le résultat en est positivement affecté. Nous avons aussi considérablement amélioré notre communication au sein de l'équipe et nos choix d'outils de travail performants et adaptés par rapport aux autres projets que nous avons pu mener lors de notre formation. Nous avons aussi compris l'importance des tests car travaillant en équipe, il est impératif que le code de chacun soit fonctionnel pour pouvoir le mettre en commun avec les autres membres et ne pas perdre de temps sur le débogage.

Outre le fait de mettre en pratique nos connaissances informatiques, ce projet nous a aussi donné l'occasion d'en acquérir de nouvelles et d'en consolider d'autres. En effet, certaines des notions que nous avons mis en pratique n'avaient été vues que théoriquement (architecture MVC par exemple), cela a donc été l'occasion de les appliquer et de mieux les comprendre.

De plus, nous avons été très sensibles à la notion de complexité algorithmique, une véritable problématique pour nous qui n'est pas toujours facile de résoudre. Cependant nous avons fait de notre mieux pour avoir un code optimisé, clair et cohérent ce qui était une vraie préoccupation pour nous.

Ce projet nous a donc beaucoup appris et nous conforte dans l'idée qu'une bonne compréhension du sujet est essentielle pour avoir une bonne conception et que notre formation nous a permis d'acquérir assez de connaissances pour mener à bien un projet de façon structurée.

ANNEXES

Livre des positions des rotors pour chaque jour

Kenngruppenheft Nr. 7


Teil A

Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel
1	DDJ	ABCK	51	GJR	FOID	101	PSJ	PQER	151	MHV	NARG
2	LWJ	AMUL	52	LTJ	YDHO	102	RCV	RGTP	152	NZO	HWOD
3	JNF	BOIJ	53	PJZ	NSGL	103	SYB	HRMT	153	POE	HXYT
4	FXO	DNDJ	54	BAU	GOHP	104	UOK	LSQM	154	QQH	RUQT
5	SMF	EHNO	55	WHE	AUPE	105	WKH	RGET	155	BQK	WUDH
6	UPL	FGAS	56	WYW	LKNG	106	KOD	UZGR	156	VLR	QWFO
7	YOP	GDHJ	57	AAJ	JAHK	107	ZDD	WKPG	157	WVT	ARJY
8	AEQ	OYVF	58	DBG	KNIT	108	DEH	JTZI	158	XZY	FPJT
9	FHJ	HTDZ	59	FOV	ZBOO	109	DWH	LXPY	159	CVZ	EXNV
10	HHL	HZNS	60	DHN	LYPO	110	HKT	IGOE	160	ANZ	NGPO
11	KOZ	JPKK	61	GXF	BNOP	111	KWH	TYOK	161	ERQ	KOON
12	NVK	EKUZ	62	JVP	NCHL	112	MKN	UBPT	162	DPL	UAMN
13	REX	ZIBS	63	NPD	AHNR	113	OQF	ILVP	163	PUB	XIYP
14	VJF	IVHX	64	QWO	MGAN	114	QJA	PHJE	164	GVD	THRS
15	XJH	YDNN	65	TTO	RZDK	115	SDX	THGN	165	JZK	INLY
16	BHL	TGHP	66	TZU	WONU	116	TVQ	NYTX	166	KQH	QXZR
17	EOJ	VYHA	67	YJK	YBNW	117	WHF	ALWR	167	NCR	EDRG
18	EDF	XHON	68	ZQS	JPLB	118	YDE	HPQO	168	QVT	OSTO
19	LGT	PBYT	69	AVX	BMCR	119	BUX	AGKT	169	QYQ	CKUT
20	OWM	RJHP	70	EVB	XQGS	120	FFN	RZYT	170	TRM	XXZW
21	QPG	SAML	71	GNV	JCDK	121	DRW	XIHS	171	ULG	QAVT
22	TOP	PCRB	72	JNX	XDNL	122	GRZ	UBZY	172	WQM	JTWU
23	ZUW	HGIM	73	LNZ	RIGX	123	JPE	TSEN	173	WQM	JTWU
24	GTT	ENTF	74	NJX	QIUW	124	LQC	NRTK	174	XFE	KSTQ
25	HTV	FUCZ	75	NTH	ZFKO	125	NDG	OYGN	175	XFE	KSTQ
26	GHN	AXSS	76	RVO	LRYF	126	PCT	IQQE	176	BHE	FIOA
27	MOD	RGNS	77	TJD	DOLE	127	RNF	HHAF	177	COB	TNPO
28	NLZ	OKRH	78	UDZ	MOND	128	YCE	GOHS	178	FMT	DCOT
29	RRK	ALIK	79	VSP	QNBV	129	YWE	WXEN	179	DMA	GNPL
30	WQO	NCYS	80	YBC	BKHI	130	ART	QTEJ	180	GDU	WVFX
31	XKW	MOEL	81	ZHE	KWOK	131	OKB	PTEO	181	JAL	TGRY
32	CAE	XSTO	82	AZB	KDZK	132	ELB	HNGD	182	RTY	NUZS
33	DOT	FENN	83	FHE	UTFA	133	QCL	BTEN	183	HMS	ITON
34	HYH	YKHY	84	HTG	TIMH	134	HBL	WOTJ	184	OOD	BLOG
35	LAL	LPMK	85	KFN	OKZU	135	KCO	XMWZ	185	QRE	SPZY
36	MOC	CFDJ	86	MTM	OHFS	136	LXM	UKNO	186	RQJ	OHXX
37	TCX	AYNE	87	ONX	YNOU	137	NGV	JPIV	187	SKN	UORG
38	UVB	WFLQ	88	QOF	LKVT	138	QBW	YVYJ	188	UBO	FVGO
39	TYT	JRPE	89	NKO	UTYG	139	SHB	SADG	189	VRO	LHNR
40	ALN	FLAI	90	VXU	WIZM	140	UTU	ONTG	190	SKN	IXKQ
41	CHM	ZERE	91	XBG	OPGZ	141	WVU	XAYF	191	SKN	GTOY
42	IGN	LEWH	92	YST	YOGZ	142	XHM	UMFP	192	OTE	BUGL
43	HON	SCZT	93	APB	TUPF	143	SDG	HYRS	193	HWT	BIGD
44	MDR	ZFOO	94	RXD	BGHN	144	AGJ	BUYO	194	LJV	UQYH
45	95	145	195	OYO	MOFU

Teil A

Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel	Nr.	Kenn- gruppe	Sprache- schlüssel
201	ANT	TCAM	251	COL	IHWL	301	KUJ	ELPD	351	PZ	
202	CCG	JSBT	252	QFX	MBZP	302	KQY	CHMO	352	RT	
203	HDR	DMJT	253	YCD	DVLK	303	VKG	ZTFI	353	YC	
204	LCP	AREN	254	MNB	GDZJ	304	LVH	MYER	354	Z	
205	OJY	SRXM	255	GFX	FVOG	305	DSZ	KYH	355		
206	WEC	JKUT	256	BAD	BCQP	306	BWZ	WXY	356		
207	YHJ	LZMQ	257	FPF	ASPD	307	MNB	KDY	357		
208	KMX	HEVR	258	RZQ	MTPX	308	ODT	GBKJ	358		
209	BRU	PHON	259	VTQ	JKCO	309	UZF	BYCQO	359		
210	JJT	RFSA	260	HTZ	QFOM	310	XAZ	QACJ	360		
211	AWY	HIMK	261	LXK	IDUP	311	YFG	GBIR	361		
212	QWE	MENU	262	RLD	SDUW	312	AYAJ	JIAT	362		
213	ODR	KONS	263	AJL	ULKO	313	HPT	KYMF	363		
214	UWS	SEKY	264	NAG	YBYQ	314	MVJ	PIAD	364		
215	QSK	PKSR	265	MJW	POCG	315	PHY	DOVJ	365		
216	TNH	WREB	266	PLB	IRFP	316	MDA	QFM	366		
217	HQE	TJMY	267	RDW	DFRX	317	KYK	SCD	367		
218	BYB	YODZ	268	XFO	GOQJ	318	NAP	SE	368		
219	QXK	MFNF	269	DNS	BTIH	319	ELL	IQ	369		
220	MSV	GTMF	270	GTR	OLKO	320	CRV	DI	370		
221	PGX	ESMY	271	XLH	CDEF	321	HPT	YC	371		
222	UCT	MDNQ	272	GOT	KWZ	322	SKD		372		
223	YKL	TAQR	273	LBD	UZVH	323	UKF		373		
224	HMF	FUSX	274	RTM	PLXR	324	KED		374		
225	DUE	TMBU	275	HRF	IOANS	325	LLT		375		
226	JAG	PXMY	276	EQW	IOBH	326	...		376		
227	LHU	OMUT	277	KCP	DROH	327	...		377		
228	ORH	NOAH	278	XTY	GNVF	328	...		378		
229	UQM	LCZS	279	DCH	SLUZ	329	...		379		
230	YFQ	HNDO	280	FLR	STFO	330	...		380		
231	ACH	IOBL	281	MFT	KJFU	331	...		381		
232	FAD	PCON	282	MMH	UKKH	332	...		382		
233	HCM	SPID	283	HFJ	XMOB	333	...		383		
234	MOQ	QORF	284	GLT	RQSE	334	...		384		
235	PTK	WRUS	285	NXM	HICK	335	...		385		
236	URZ	TFOD	286	CFH	CTXM	336	...		386		
237	ENO	MMIR	287	DXC	AFIK	337	...		387		
238	ATV	PLMR	288	HUD	GVJO	338	...		388		
239	QNR	BFAL	289	QOC	MYOJ	339	...		389		
240	HJB	NILK	290	QAS	KDFT	340	...		390		
241	KXJ	ILBN	291	ETE	SCG	341	...		391		
242	KXN	GOOU	292	WUS	QFZ	342	...		392		
243	QMH	EMBE	293	FWH	ME	343	...		393		
244	QEQ	KEEP	294	HRD	QVZ	344	...		394		
245	YHV	WFOO	295	DQV	Z	345	...		395		
246	JMK	ORIS	296	346	...		396		

Github : partage du projet entre les membres de l'équipe

 **Marianna-dl / EnigmaProject**

Unwatch 3

Star 0

Fork 0

Description

Short description of this repository

Website

Website for this repository (optional)

Save or Cancel

61 commits

1 branch

0 releases

3 contributors

branch: master

EnigmaProject / +

opti vue+lien plug controleur+correction bu plugboard

Marianna-dl authored 2 days ago

latest commit 6d671792d4

Conception	update maquette interface	22 days ago
Gestion de projet	update rapport + diagramme	18 days ago
Mock	update + rajout scroll	9 days ago
Projet	opti vue+lien plug controleur+correction bu plugboard	2 days ago
Rapport	ajout cryptanalyse rapport	5 days ago
tests observer	test observer et observable	22 days ago
Enigma.jar	add enigma.jar	9 days ago

Help people interested in this repository understand your project by adding a README!

Add a README

<> Code

Issues 0

Pull Requests 0

Wiki

Pulse

Graphs

Settings

HTTPS clone URL

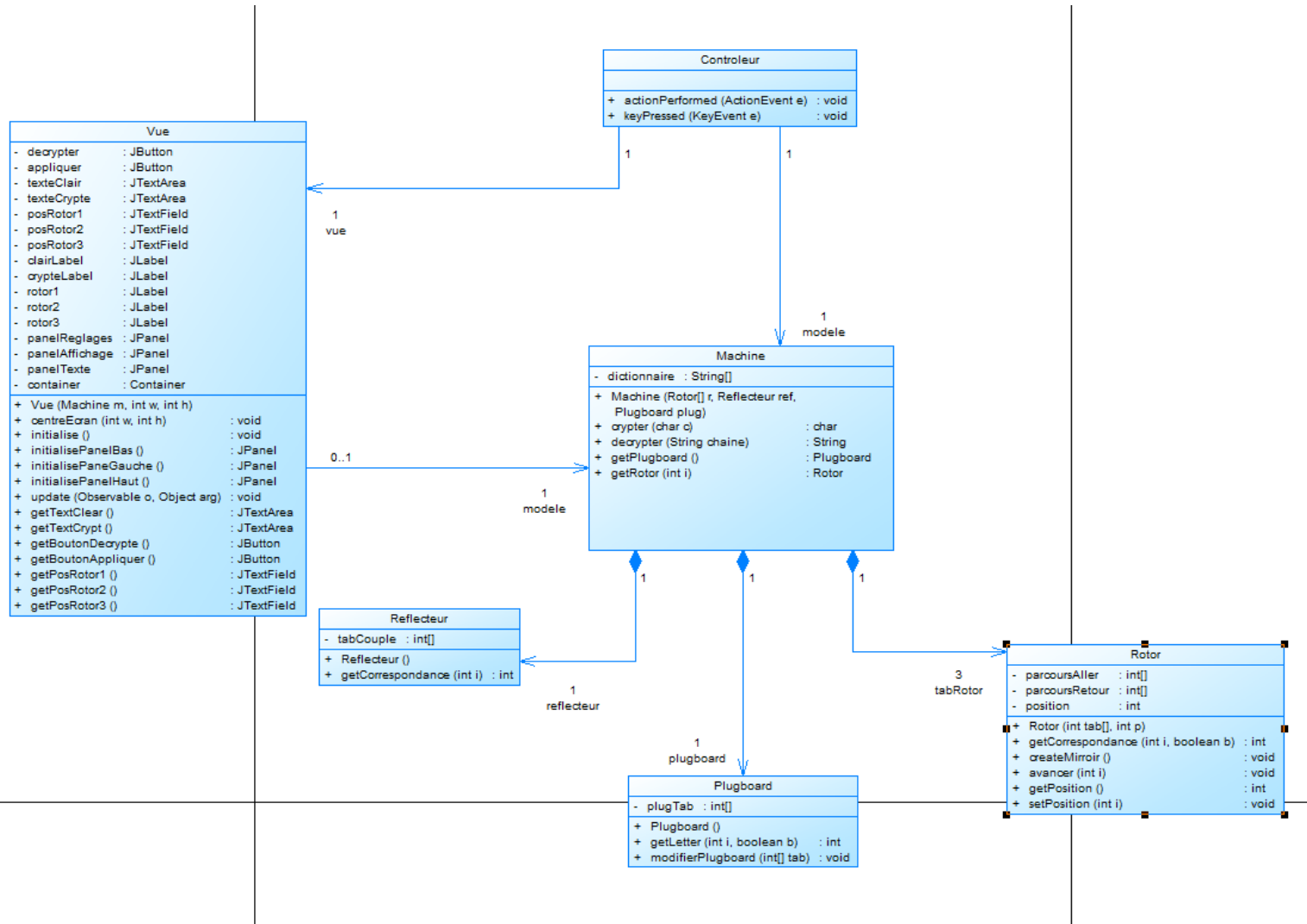
https://github.com/I

You can clone with HTTPS, SSH, or Subversion.

Clone in Desktop

Download ZIP

Conception UML


[Conception UML \(PDF\)](#)
[Diagramme de Gantt \(PDF\)](#)

Sources

https://www.youtube.com/watch?v=G2_Q9FoD-oQ par « numberphile »

https://www.youtube.com/watch?v=7dpFeXV_hqs par « e-penser »

https://interstices.info/encart.jsp?id=c_9752&encart=0&size=790,700

<http://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/enigmafonc>