

Projet Enigma

2014-2015

Naïm Kissi

Robin Trouve

Marianna De Lima



Plan

- ▀ Enigma: Machine de cryptage
 - ▀ Les rotors
 - ▀ Le plugboard
 - ▀ Le réflecteur
- ▀ Enigma: Simulation informatique
 - ▀ Organisation du projet
 - ▀ Logique de fonctionnement
 - ▀ Difficultés et solutions retenues

Les rotors



- Au nombre de trois parmi 5
- Forme cylindrique et fixé sur un axe où ils peuvent tourner
- Forme cylindrique et fixé sur un axe où ils peuvent tourner
- Une lettre ne sera pas cryptée deux fois par la même lettre

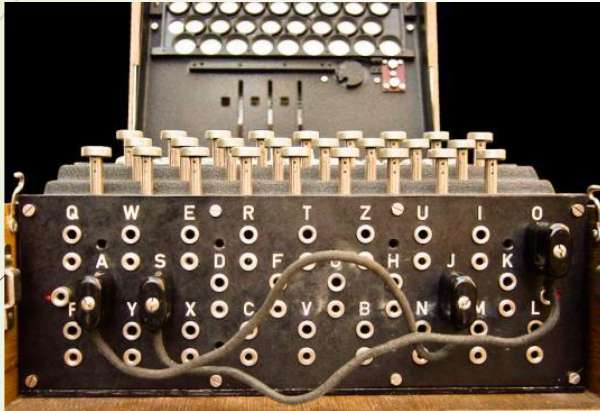
Nombre de possibilités:

$$5 \times 4 \times 3 = 60 \quad 26^3 = 17\,576$$

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

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

Le Plugboard



- Tableau de connexion situé devant la machine
- Permet de permuter deux lettres entre elles
- Il offre le plus de possibilité de cryptage

Nombre de possibilités du
plugboard:

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

Nombre de possibilités totale:

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

Le réflecteur



- Rend le cryptage réversible
- Plus besoin d'avoir une machine pour crypter et une autre pour décrypter
- « A » cryptée en « B » alors « B » sera décryptée en « A »
- Empêche alors toute lettre d'être cryptée par elle-même
- Ne rajoute pas de possibilités de cryptage

Organisation du projet

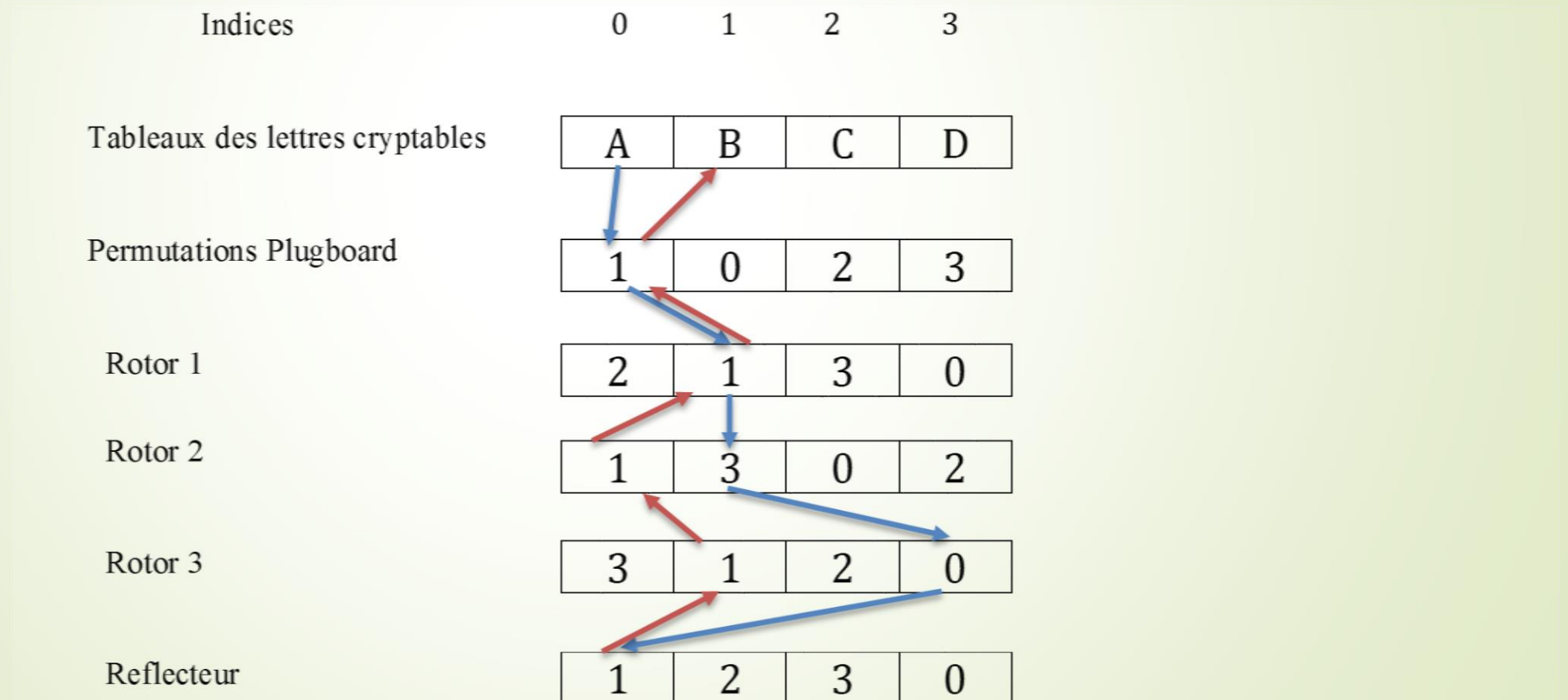
- Compréhension du sujet et du fonctionnement d'Enigma
- Mise en accord sur les différents outils (Java, MVC)
- Création du diagramme de Gantt



- Conception UML
- Répartition des tâches:
 - Model : cœur de l'application
 - View : interface utilisateur
 - Controller : verification des données saisies

Logique de fonctionnement

- Rotors = tableaux d'entrées/sorties





Difficultés rencontrées et solution retenues

Difficultés	Solutions
Complexité algorithmique: Temps de calcul	Création de tableaux « miroirs »
Interface graphique: Non responsive (adaptative)	Création interface v2.0 avec Java FX et Scene Builder
Méthode « Decrypter » Décryptage long et coûteux	Création d'une classe à part. - méthode de décryptage naïve - Méthode basée sur indice de coïncidence



Bilan

- Nouvelles connaissances en cryptographie
 - Fort intérêt pour la cryptanalyse
 - Application de nos connaissances en informatique et en gestion de projet
 - Envie de continuer le projet
- 