



Fiche professeur 1/6

Comment sont cryptées les données avant d'être communiquées ?

Thème n°2 et 3

Cycle 4

Technologie Cycle 4

Séance 3

Sources Traam
Académie de Nancy-Metz

Compétences disciplinaires de Technologie : « Thème 2 et 3 » :

Compétences de fin de cycle	Repères de progressivité : 4 ^e
Comprendre et modifier un programme associé à une fonctionnalité d'un objet ou d'un système technique	<p>Analyser les données et en déduire des modifications à apporter au programme</p> <p>Compléter un programme pour répondre à une fonctionnalité d'un OST</p> <p>Tester et valider, dans un environnement simulé ou réel, une modification du programme</p>



Introduction : « LA MACHINE ENIGMA »

La machine Enigma était un appareil de codage électromécanique utilisé principalement par l'Allemagne nazie pendant la Seconde Guerre mondiale pour sécuriser ses communications. Elle a joué un rôle clé dans le secret des messages militaires, et sa décryptation par les Alliés a constitué un tournant décisif dans le conflit.



Fonctionnement de la machine Enigma :

1. Les rotors :

L'élément clé de la machine Enigma était son système de **rotors**. Chaque rotor était un disque métallique comportant **26 positions** (une pour chaque lettre de l'alphabet). Chaque rotor était câblé différemment à l'intérieur, ce qui assurait que chaque lettre soit codée de manière unique. Il y avait plusieurs rotors, et leur arrangement pouvait être changé, ce qui offrait une immense variété de combinaisons. En général, la machine **utilisait de 3 à 5 rotors** selon le modèle.



2. Le clavier et la connexion des lettres :



L'opérateur tapait une lettre sur le clavier de la machine, et celle-ci passait à travers les rotors. Les rotors modifiaient le signal, et la lettre était ensuite codée en une autre lettre, qui s'affichait sur un tableau de lampes. La connexion des lettres changeait à chaque pression sur une touche, créant un effet de substitution complexe.

3. Le réflecteur :

Un autre composant important était le **réflecteur**. Après que le signal ait traversé les rotors, il était renvoyé par le réflecteur à travers les rotors dans la direction inverse. Cela signifiait que chaque lettre était encodée de manière réversible, mais cela compliquait la décryptation, car il était impossible de revenir à la lettre initiale sans connaître exactement la configuration des rotors.





Fiche professeur 2/6

Comment sont cryptées les données avant d'être communiquées ?

Thème n°2 et 3

Cycle 4

Technologie Cycle 4

Séance 3

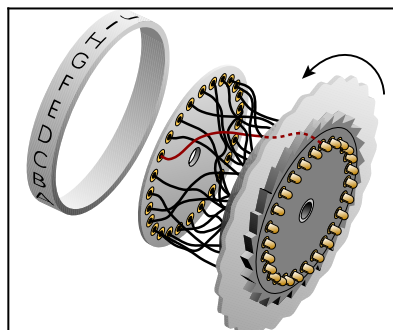
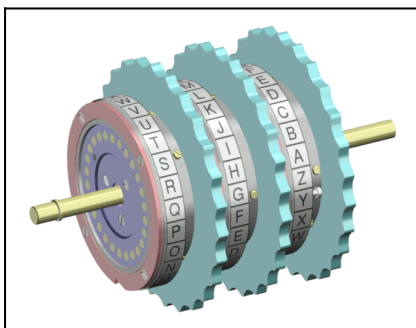
Sources Traam
Académie de Nancy-Metz

4. La roue d'entrée et la roue de sortie :

Ces éléments permettent la circulation du courant à travers la machine, ce qui assure que chaque lettre est transformée de façon unique.,

5. Les réglages et clés de sécurité :

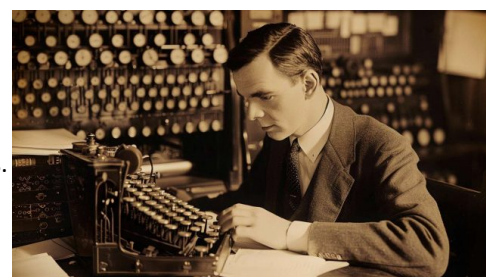
La sécurité d'Enigma reposait sur les réglages quotidiens des rotors, leur ordre, les positions de départ et les câblages des connexions internes. Chaque jour, un code maître dictait la configuration des machines. Cela signifiait qu'il y avait un nombre de configurations théoriquement **infini** que les Alliés devaient découvrir pour briser le code.



<https://www.youtube.com/watch?v=ybkkiGtJmkM>

6. Casse du code Enigma :

Le travail des cryptanalystes alliés, particulièrement à **Bletchley Park** en Grande-Bretagne, a été crucial pour déchiffrer les messages secrets de la machine Enigma. Le mathématicien **Alan Turing** et ses collègues ont conçu une machine, la **bombe** (une sorte de précurseur de l'ordinateur moderne), qui permettait de tester rapidement les différentes combinaisons des rotors. Cela a permis de casser les codes à une vitesse suffisante pour intercepter des communications cruciales pendant la guerre.



Enigma est donc un exemple de système de cryptage très avancé pour l'époque, mais sa vulnérabilité résidait dans la répétition de certains codes et dans l'erreur humaine. Sa décryptation a permis aux Alliés de lire une grande quantité de communications allemandes, contribuant à la victoire sur le IIIe Reich.

Extrait du film « Imitation Game » :

<https://ladigitale.dev/digiview/#/v/689f7ce50b886>



Explication du cylindre enigma :

<https://ladigitale.dev/digiview/#/v/68a053b841020>





Fiche professeur 3/6

Comment sont cryptées les données avant d'être communiquées ?

Thème n°2 et 3

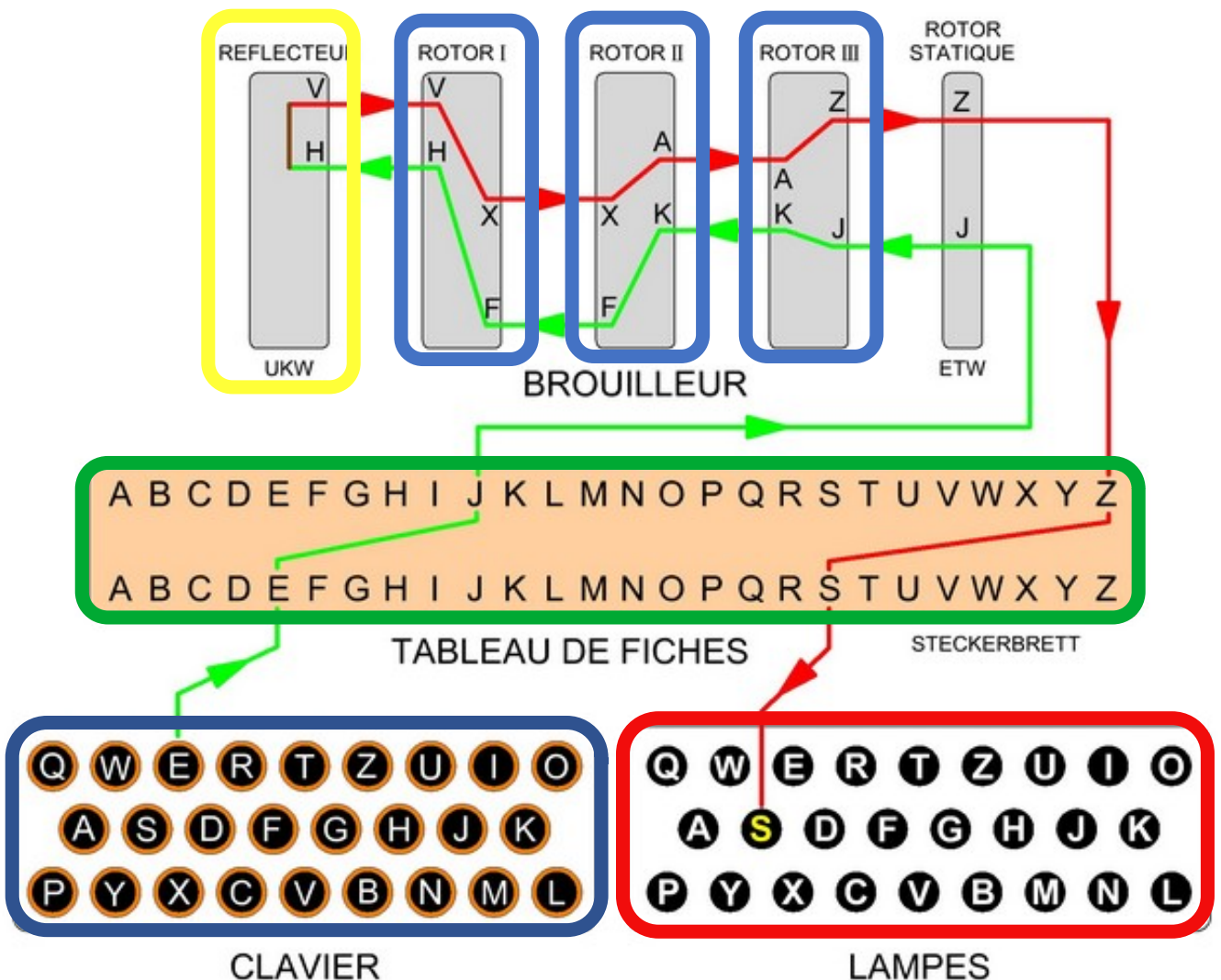
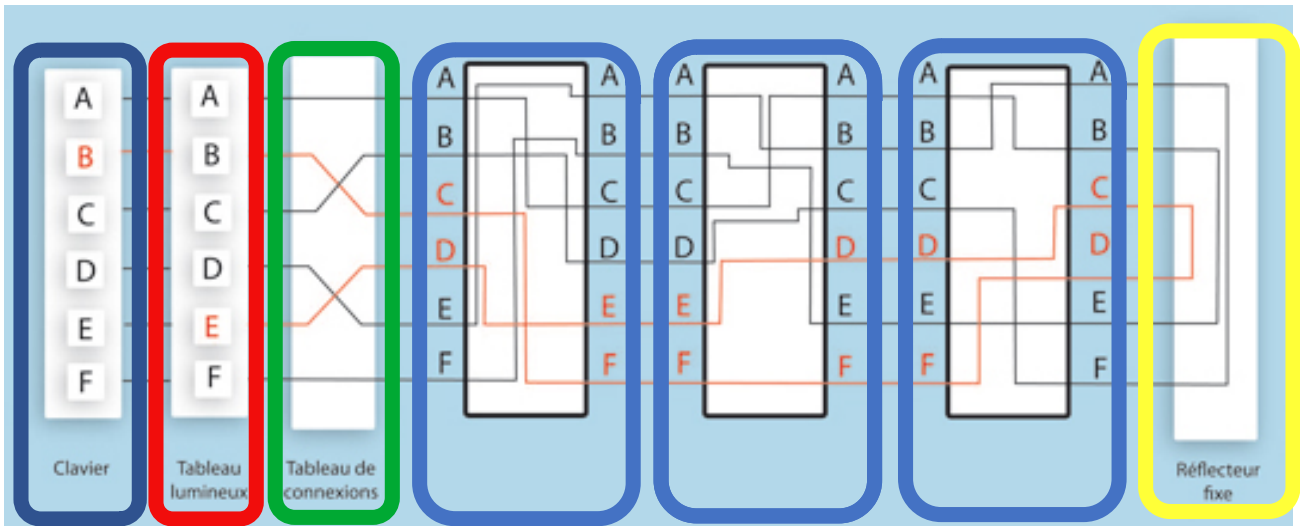
Cycle 4


Technologie Cycle 4

Séance 3

Sources Traam
Académie de Nancy-Metz

Le principe de fonctionnement :



 <p>ACADÉMIE DE NORMANDIE Liberté Égalité Fraternité</p>	<h1 style="color: red;">Fiche professeur 4/6</h1> <h2 style="color: green;">Comment sont cryptées les données avant d'être communiquées ?</h2> <p>Thème n°2 et 3</p>	Cycle 4
		Technologie Cycle 4
		Séance 3
		Sources Traam Académie de Nancy-Metz

Voici 5 questions sur le film « *Imitation Game* » (aussi appelé *Enigma*) :

1. Quelle est la mission principale d'Alan Turing et de son équipe pendant la Seconde Guerre mondiale dans le film ?

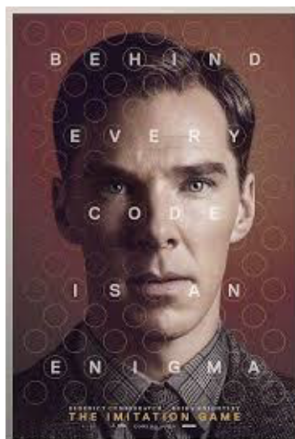
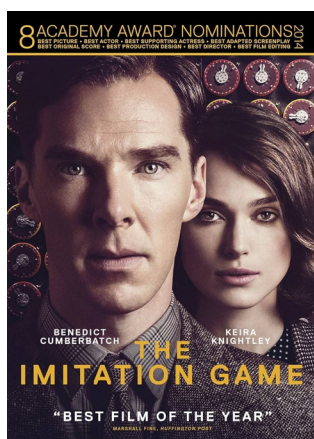
La mission principale d'Alan Turing et de son équipe est de déchiffrer les messages codés de la machine Enigma, utilisée par les nazis pour communiquer en toute sécurité. Turing et son équipe cherchent à créer un moyen efficace pour briser ce code afin de fournir des informations cruciales aux alliés, ce qui pourrait potentiellement changer le cours de la guerre.

2. Pourquoi le film porte-t-il le nom *Imitation Game*, et comment ce concept est-il lié à l'intelligence artificielle ?

Le film s'intitule "Imitation Game" en référence au test de Turing, une expérience de pensée proposée par Alan Turing pour évaluer si une machine peut reproduire un comportement intelligent similaire à celui d'un humain. Ce concept est lié à l'intelligence artificielle car il pose la question de la capacité des machines à penser et à interagir de manière autonome, un sujet central dans le développement de l'IA.

3. Comment le film montre-t-il l'importance du travail de Turing pour briser le code de la machine Enigma ?

Le film illustre l'importance du travail de Turing en mettant en avant les nombreux défis et obstacles qu'il rencontre, ainsi que sa détermination à résoudre le problème. À travers ses calculs complexes et sa vision innovante, Turing parvient à concevoir une machine capable de décoder les messages Enigma, montrant ainsi que son travail sauve des vies et contribue de manière significative à l'effort de guerre.





Fiche professeur 4/6

Comment sont cryptées les données avant d'être communiquées ?

Thème n°2 et 3

Cycle 4

Technologie Cycle 4

Séance 3

Sources Traam
Académie de Nancy-Metz

4. Quel est le rôle de la machine "Christopher" dans le film, et comment aide-t-elle à résoudre le problème de la cryptanalyse ?

La machine "Christopher" est une création de Turing qui représente une avancée technologique majeure dans le domaine de la cryptanalyse. Elle est conçue pour automatiser le processus de déchiffrement des messages codés par Enigma, permettant ainsi de traiter un grand nombre de combinaisons possibles plus rapidement qu'un humain. Christopher aide Turing et son équipe à analyser et à déchiffrer les messages, rendant le processus beaucoup plus efficace.

5. En quoi le film souligne-t-il la tragédie de la vie de Turing, notamment après la fin de la guerre et ses difficultés personnelles liées à la loi sur l'homosexualité ?

Le film souligne la tragédie de la vie de Turing en montrant comment, après avoir joué un rôle crucial dans la victoire des alliés, il est confronté à la discrimination et à la persécution en raison de son homosexualité, qui était illégale en Grande-Bretagne à l'époque. Turing subit une castration chimique comme alternative à l'emprisonnement et finit par se suicider, ce qui met en lumière l'injustice et la souffrance qu'il a endurées malgré ses contributions inestimables à la société.

6. De combien de temps est-ce que l'on estime que cette machine a écourté la guerre ?

On estime que le travail d'Alan Turing et de son équipe, notamment grâce à la machine qu'ils ont développée pour déchiffrer les codes d'Enigma, a permis d'écourter la Seconde Guerre mondiale d'environ deux à quatre ans. Les informations obtenues grâce à la déchiffrement des messages ont aidé les Alliés à prendre des décisions stratégiques cruciales, sauvant ainsi de nombreuses vies et modifiant le cours du conflit.

7. On estime à combien le nombre de personnes sauvées ?

On estime que le travail d'Alan Turing et de son équipe a permis de sauver environ 14 millions de vies pendant la Seconde Guerre mondiale.

8. Combien de machines ENIGMA ont été utilisées par les Allemands ?

Les Allemands ont utilisé plusieurs milliers de machines Enigma pendant la Seconde Guerre mondiale. On estime qu'environ 30 000 machines Enigma ont été produites et utilisées par les forces armées allemandes, y compris l'armée de terre (Heer), la marine (Kriegsmarine) et l'aviation (Luftwaffe). Chacune de ces machines était utilisée pour sécuriser les communications militaires, ce qui compliquait considérablement les efforts de déchiffrement des Alliés.

9. Trouver le prix d'une machine vendue aux enchères ? **425 000 dollars**



Fiche professeur 5/6

Comment sont cryptées les données
avant d'être communiquées ?

Thème n°2 et 3

Cycle 4

Technologie Cycle 4

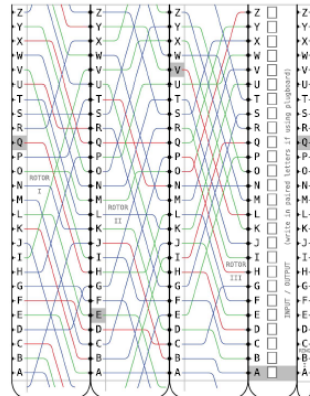
Séance 3

Sources Traam
Académie de Nancy-Metz

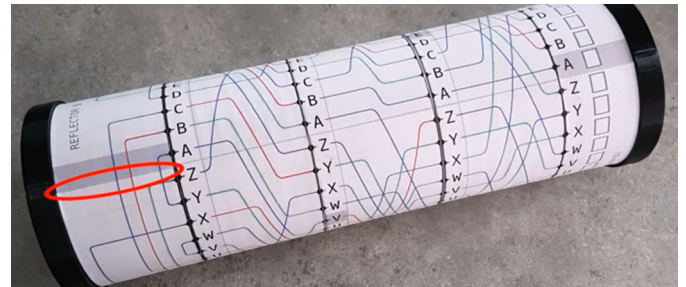
Réaliser la maquette en papier de la machine « Enigma » selon les consignes de la vidéo :



+



=



Vidéo d'explication de la maquette en papier :

<https://www.youtube.com/watch?app=desktop&v=GGLU0TOyFBo&t=579s>



Site web permettant de vérifier le codage :

<https://enigma.virtualcolossus.co.uk/VirtualEnigma/>
<https://www.101computing.net/enigma/enigma-M3.html>

Le site à utiliser !

<https://curioandrelie.com/cgi-bin/enigma.py>

En utilisant votre maquette en papier selon la configuration des rotors en position A B et C :

Que donne la lettre O ? : réponse la lettre J

Vérifier avec le site : <https://curioandrelie.com/cgi-bin/enigma.py>

