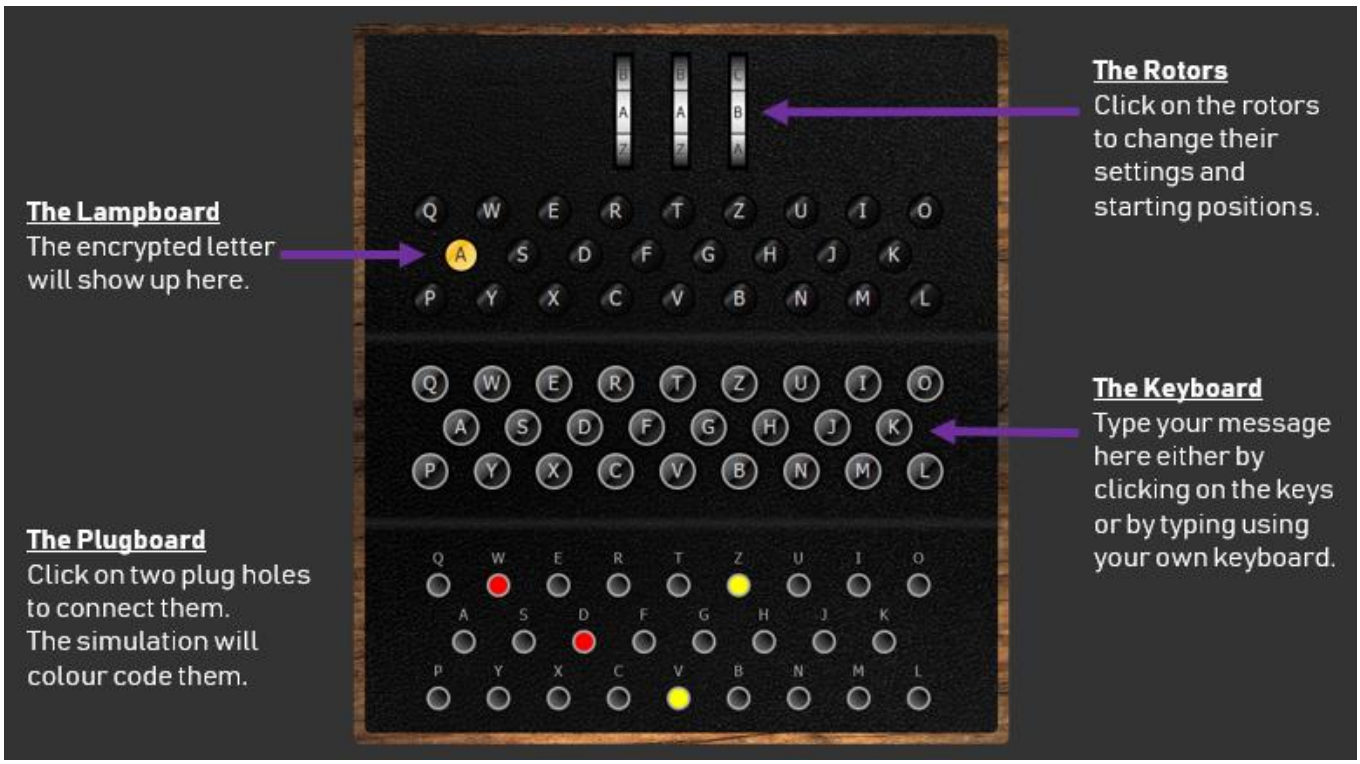
À l'intérieur d'Enigma

La machine énigme est une machine de cryptage assez complexe qui se compose de quatre sections principales :



1) Le clavier (keyboard) :

Le clavier est utilisé pour récupérer l'entrée utilisateur. La machine Enigma est une machine de cryptage symétrique. Ce qui signifie qu'elle peut être utilisée à la fois pour crypter ou décrypter un message en utilisant les mêmes paramètres. Le clavier est donc utilisé pour saisir soit le texte en clair qui doit être chiffré, soit le texte chiffré qui doit être déchiffré.

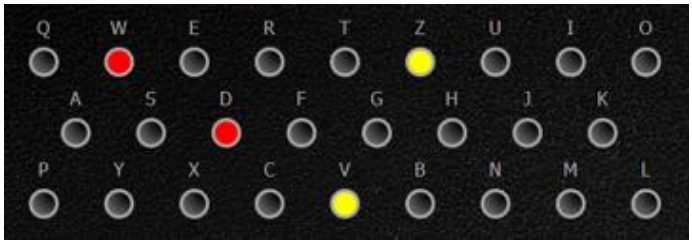
Le clavier se compose de 26 touches, une pour chaque lettre de l'alphabet. Cela signifie que les messages cryptés seront joints sans espaces ni signes de ponctuation.

Le clavier commence par les lettres QWERTZ au lieu de QWERTY. Cela est dû au fait que dans la langue allemande, la lettre Z est plus souvent utilisée que la lettre Y.

2) Le panneau de connexion (plugboard) :

Une fois qu'une touche est enfoncée sur le clavier, la lettre passe par le plugboard qui fournit la première étape du processus de cryptage. Il est basé sur les principes d'un chiffrement de substitution.

Pour configurer les claviers, des fils courts sont utilisés pour connecter des paires de lettres qui seront permutées. Par exemple, sur l'image ci-dessous, la lettre W sera remplacée par un D et la lettre D par un W car un fil (rouge) est utilisé pour connecter ces deux lettres. De même, la lettre V deviendra la lettre Z et Z deviendra V.



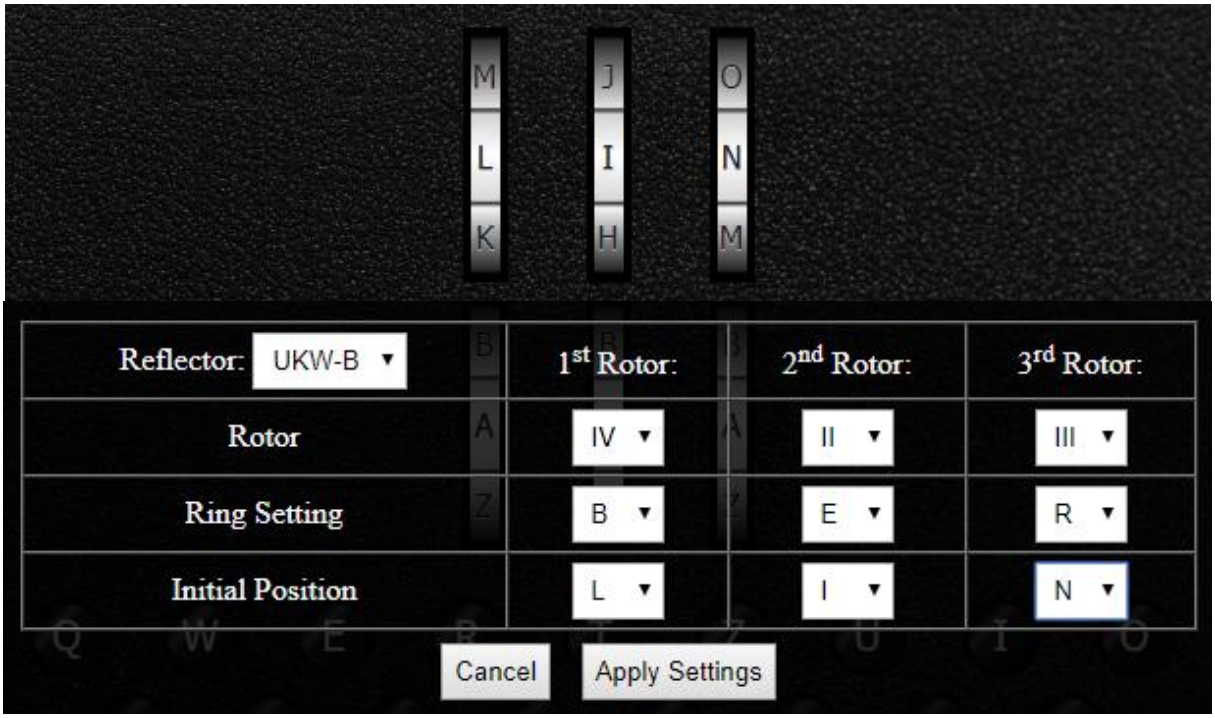
Dans un livre de codes, les paramètres du panneau de connexion seraient enregistrés comme suit : DW VZ

3) Les rotors :

Après le plugboard, la lettre parcourt les trois rotors dans l'ordre (de droite à gauche), chacun d'eux la modifiant en utilisant une combinaison de chiffrement par transposition. Sur l'Enigma M3, il y a possibilité d'utiliser trois rotors parmi les cinq disponibles. Chaque rotor est identifié à l'aide d'un chiffre romain de I à V. Cela fournit quelques paramètres de la machine Enigma : quels rotors utiliser et dans quel ordre les positionner. Dans un livre de codes, ce réglage serait enregistré comme IV II III (rotors gauche, moyen et droit).

Chacun des cinq rotors crypte la lettre différemment en utilisant un chiffrement de transposition et peut être connecté dans la machine Enigma avec différentes configurations internes. Un autre réglage est la position initiale des rotors : lettre définie sur chaque rotor pour commencer (par exemple A / B / C / ... / Z parfois enregistré dans un livre de codes à l'aide de nombres (01 pour A, 02 pour B jusqu'à 26 pour Z). Sur une machine Enigma, vous pouvez changer la position des rotors en tournant les trois roues.

Différentes versions d'Enigma (par exemple M4) comprenaient quatre rotors, ce qui augmentait encore davantage le processus de cryptage et le nombre de paramètres possibles.



Ce qui rend le code Enigma particulièrement difficile à déchiffrer, c'est qu'à chaque fois qu'une touche est enfoncée, le rotor de droite tourne d'une lettre. Ce qui signifie que les paramètres de cryptage changent constamment pour chaque lettre d'un message. Cela signifie également qu'une seule lettre en clair serait chiffrée différemment en fonction de sa position dans le message.

Les rotors sont également connectés les uns aux autres de sorte que lorsque le rotor positionné à droite atteint une lettre spécifique, il déclenche le rotor du milieu pour qu'il tourne d'une lettre. De même, lorsque le rotor au milieu atteint une lettre spécifique, il déclenche le rotor de gauche pour qu'il tourne d'une lettre.

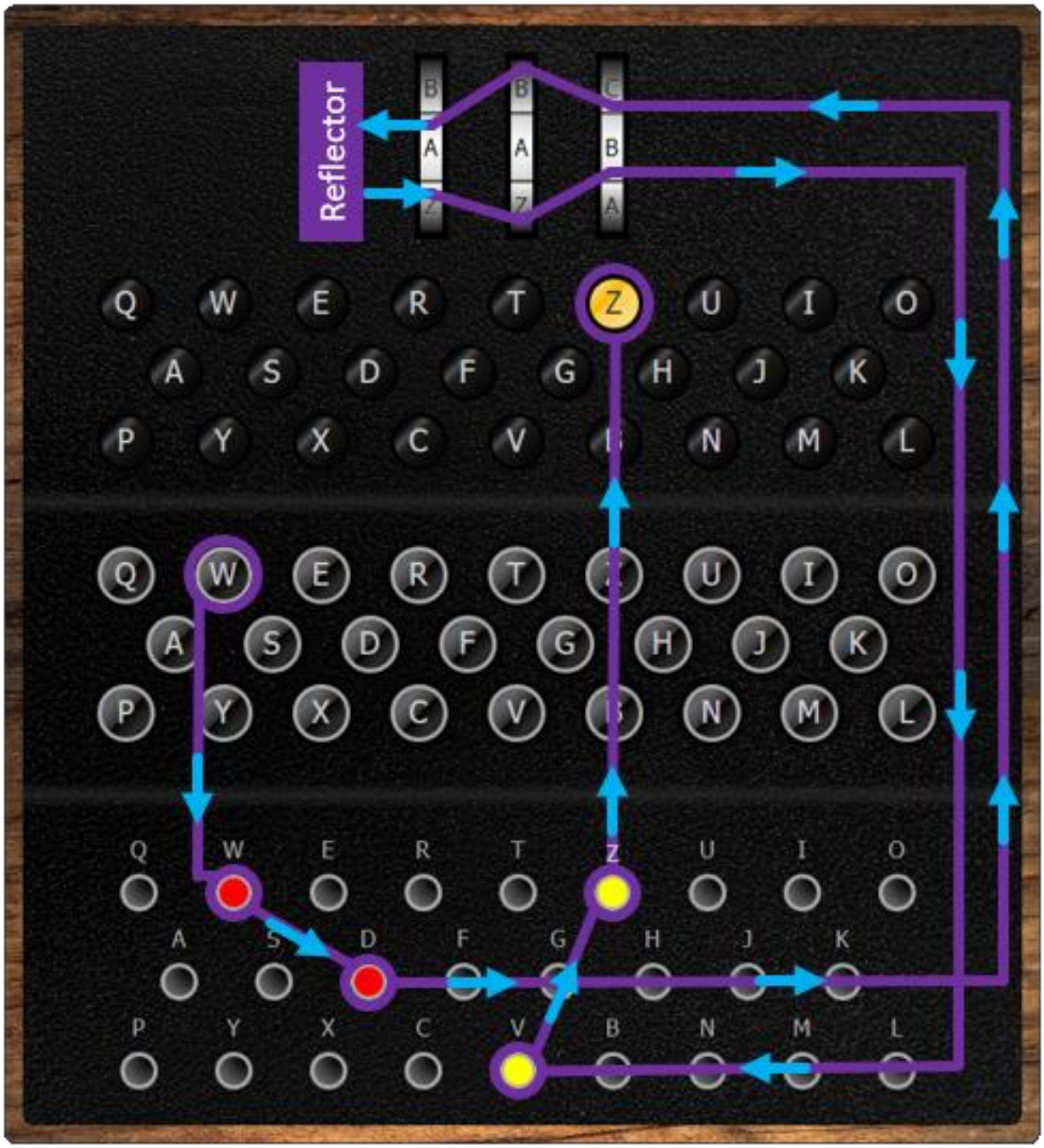
Le réflecteur :

Le réflecteur est un autre type de rotor à l'intérieur de la machine. Une fois que la lettre a traversé les trois rotors de droite à gauche, le réflecteur reflétera le courant électrique à travers les rotors, envoyant la lettre cryptée à travers les rotors de gauche à droite pour 3 autres étapes de cryptage,

puis à nouveau à travers le tableau de connexion pour un chiffre de substitution final. Lors du passage dans le réflecteur, une permutation est également appliquée à la lettre.

Différentes versions de réflecteurs ont été utilisées sur différentes versions des machines Enigma. Chaque réflecteur appliquerait un chiffre de permutation différent. Les machines Enigma M3 étaient équipées d'un réflecteur UKW-B ou UKW-C.

Le diagramme ci-dessous montre le parcours d'une lettre à travers le processus de cryptage d'une Enigma M3.



4) Le panneau de lampes (lampboard) :

Le lampboard est la dernière étape du processus de cryptage et est utilisé pour afficher la sortie (lettre cryptée). Il se compose de 26 ampoules, une pour chaque lettre de l'alphabet.