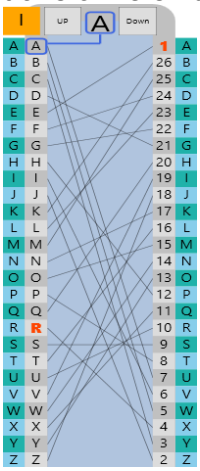
Le chiffrement d’enigma

Ce cours décrit l’aspect technique du code d’enigma, si vous voulez voir un récapitulatif avec plus de contexte je vous invite à regarder la fiche n°6.

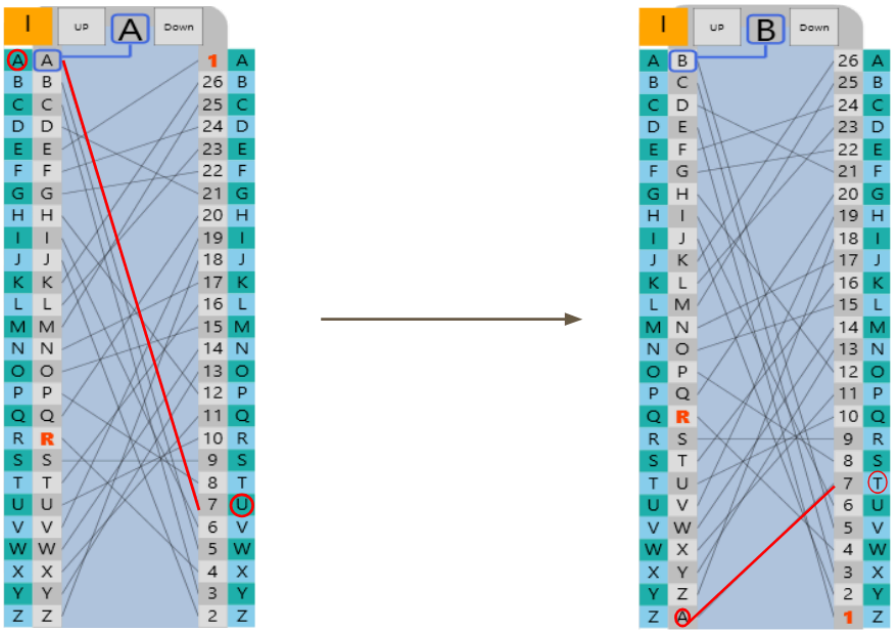
Attention je vais ici présenter une des machines enigma sachez qu’il en existe plusieurs versions avec plus de rotors ou de câbles de branchement par exemple.

1. Les rotors

Qu’est ce qu’un rotor? Un rotor applique une substitution monoalphabétique (une lettre transformé en une autre), comme ici:



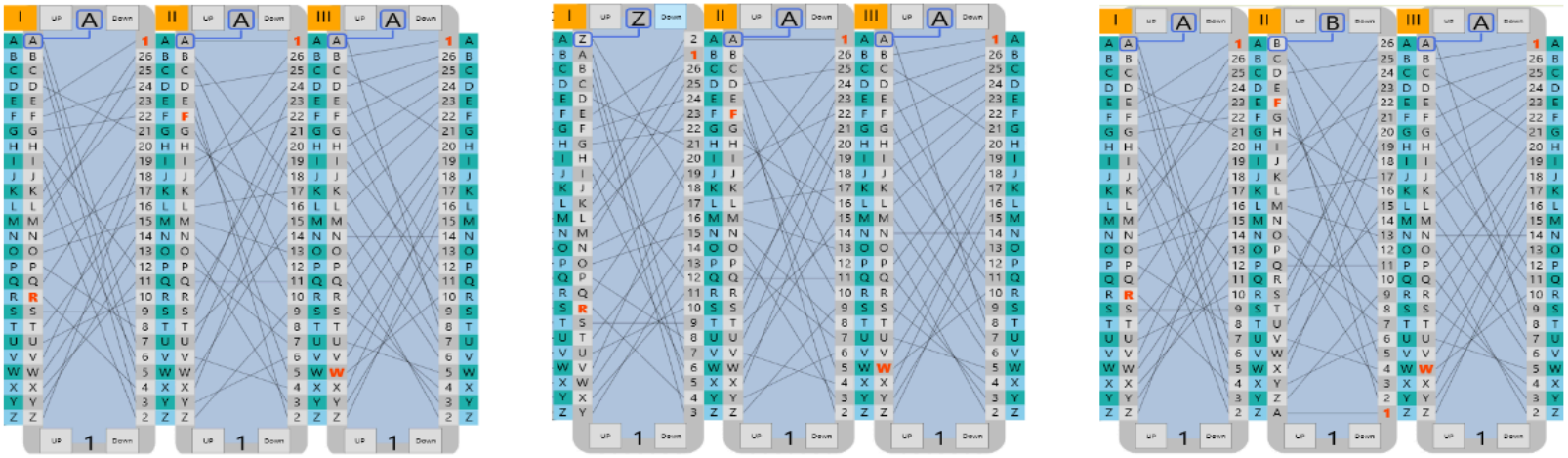
Ensuite, à chaque fois que l’on chiffre une lettre, le rotor se décale d’un cran:



On a donc 26 alphabet chiffré.

La machine enigma comporte 3 rotor différent , qui fonctionnent sur le même principe à un détail près: le rotor n°2 ne tournera qu'après un tour complet du premier :

Position 0 Position 25 Position 26

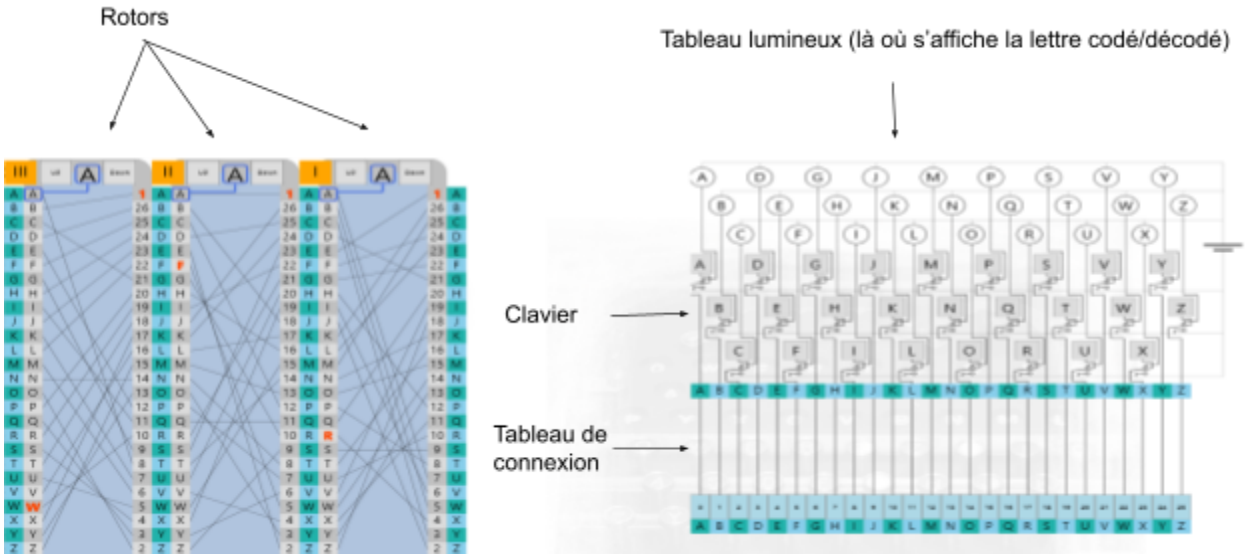


Les rotors définissent donc 26x26x26 alphabets chiffré différent, soit 17 576 possibilités

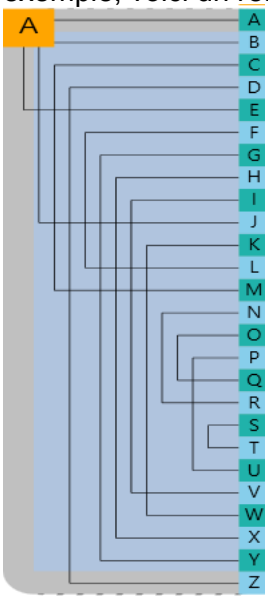
De plus, il y a 5 rotors qui peuvent être positionnés et interchangés dans différentes positions: Dans l'exemple, j'ai utilisé les rotors I, II, et III dans cette position. J'aurais pu utiliser les rotors II, V et IV par exemple. Cela ajoute 5x4x3 possibilités, soit 60.

2. Le tableau de connexion et le réflecteur

Le tableau de connexion est l'élément le plus important et le plus simple d'enigma. L'opérateur a 10 câbles qui permettent de permuter 2 lettres entre elles: par exemple A avec B. Cela parrait tout simple, mais ajoute 150 738 274 937 250 possibilités.
Pour le moment, enigma ressemble à cela :



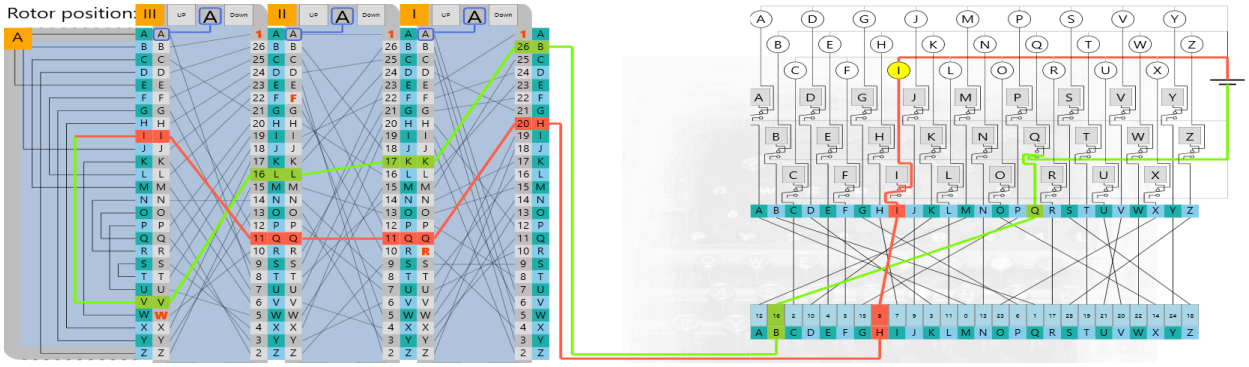
On tape une lettre sur le clavier, qui passe par le tableau de connexion , puis par les rotors et enfin sur le tableau lumineux. Pour coder , c'est simple. Mais pour décoder? Il faudrait passer la lettre dans les rotors en premier, et cela nécessiterait 2 claviers. A la place, le réflecteur a été ajouté. C'est une pièce fixe , qui transforme une lettre en une autre et inversement. Par exemple, voici un réflecteur:



Il permet que la lettre chiffrée suive le chemin tableau de connexion-rotors-réflecteur-rotor-tableau de connexion dans le codage et le décryptage.

3. Enigma finale

L'enigma finale ressemble donc à ceci: (avec la lettre q codé comme exemple):



Avec un nombre immense de possibilités de clef : **158 962 555 217 826 360 000** !(non ce n'est pas une factorielle)

Voici donc la fin de ce cours, j'espère qu'il vous a plu et qu'il vous a appris des choses!