"ENIGMA"

Enigma est une machine de cryptage qui a joué un rôle capital dans les affaires d'espionnage au cours la seconde guerre mondiale. Toutes les communications des nazis passaient par cette machine et en ressortaient sous la forme d'un charabia incompréhensible. Le codage d'*Enigma* a longtemps eu la réputation d'être inviolable. En raison de cette machine impassible, les soldats alliés tombaient les uns après les autres. Or, grâce à des opérations audacieuses et aussi à un peu de diplomatie, les Alliés ont pu confectionner un appareil correspondant à l'équipement de codage des ennemis. Cependant, celui-ci, en tant que tel, n'était d'aucune utilité : il a fallu qu'un grand mathématicien du nom d'Alan Turing fasse bénéficier les Alliés de son génie en cryptographie. Nous allons voir pourquoi le simple fait de posséder un modèle d'*Enigma* n'était pas suffisant pour décrypter les missives allemandes. Pour cela, nous allons détailler le principe de son fonctionnement. Lançons-nous à la découverte de cet objet magnifique :

1) A la fin de ce document, vous trouverez une annexe. Découpez le "rotor" en suivant les traits de coupe (notez que la précision est requise en matière de cryptographie: pour votre confort, veillez à ne pas laisser de résidus de pointillés).
Pour les connaisseurs de logiciels de montage qui voudraient procéder aux manipulations de manière virtuelle, cela est parfaitement possible : des fichiers PNG sont également à disposition.

2) Posez le "rotor" entre l'alphabet et le petit cercle du milieu : vous constatez qu'un signal part de chaque lettre et conduit à une autre lettre. Faites coulisser circulairement le "rotor" le long de l'alphabet et positionnez-le de manière à ce que les deux repères (flèches) soient réunis. Ne touchez plus à rien : pour comprendre le principe, vous allez tout d'abord procéder au codage d'un mot en vous servant des correspondances indiquées.

3) Essayez de coder "MISSISSIPPI". Qu'obtenez-vous ? Un mot dont l'apparence est tout à fait similaire au mot initial (en particulier les répétitions de lettres). Quelques instants de réflexion suffiraient pour associer aux lettres codées les lettres initiales respectives, et cela même si l'on n'est pas en possession de la machine. La facilité du décryptage provient du fait qu'une lettre est toujours codée de la même manière (exemple : dans "MISSISSIPPI" on retrouve bien quatre W et quatre C, respectivement associés aux quatre I et aux quatre S).

4) C'est ici que le twist intéressant intervient. Imaginons qu'après chaque opération de codage d'une lettre, on fasse tourner le rotor d'un cran. Essayons. Veillez à positionner la flèche indiquée sur le rotor en face de la flèche indiquée sur l'alphabet. Il s'agit toujours de coder le mot "MISSISSIPPI", mais, cette fois-ci, vous allez procéder à la rotation d'un cran (sens horaire) du "rotor" à chaque fois que vous aurez codé une lettre (aide*). Vous conviendrez que dans ces

conditions, il est impossible d'associer intuitivement une lettre à une autre : ni les quatre I, ni les quatre S ne sont codés de la même manière, ils sont différents à chaque occurence.

5) Vous venez de découvrir le principe d'*Enigma*. C'est aussi simple que cela. Ou presque. En réalité, la machine ne comportait pas seulement un emplacement à "rotor", mais trois. Et les nazis ont eu jusqu'à huit rotors à leur disposition qu'ils pouvaient insérer dans l'un ou l'autre des trois emplacements. De plus, n'oublions pas que la position initiale de chaque rotor entrait également en jeu. Ainsi, le nombre de combinaisons était astronomique. Chaque jour, à la même heure, les nazis attribuaient une nouvelle configuration, applicable immédiatement sur toutes leurs machines à travers le monde.

6) Nous entrons dans le vif du sujet : le décryptage d'un message. Nous ne verrons bien sûr qu'un aspect simplifié d'un processus qui fut en vérité long et laborieux, celui auquel les équipes d'Alan Turing devaient se livrer quotidiennement.
Le point de départ fut la découverte d'une faille terrible dans le fonctionnement d'*Enigma*. D'une part, comme vous l'avez sans doute remarqué, une lettre ne peut jamais être codée par elle-même. À cela s'ajoute autre chose : les allemands, très disciplinés, envoyaient chaque jour un rapport météo. Les Alliés, ayant appris cela, surent qu'ils devaient chercher l'emplacement du mot "*Wetterbericht*" qui signifie "rapport météo" en Allemand. Ils entreprirent donc de confronter ce mot avec les séquences de lettres incompréhensibles qu'ils devaient décrypter. Il suffirait d'identifier, dans le texte à décrypter, un passage de 13 lettres dans lequel aucune des lettres ne correspondrait aux lettres du mot "Wetterbericht". De cette manière, les Alliés pouvaient déterminer la position des "rotors" lors du codage de ce message. Vous n'avez pas tout suivi ? Ce n'est pas grave. Reprenons étape par étape :

7) Les services secrets vous ont fait parvenir le message suivant, vous êtes chargé de le décrypter :

```
RFUOXLHRMDCFHPUC  ///  CZVTIGMCQAIFKWBWLPSNKJHWGWOUXLNPZE
```

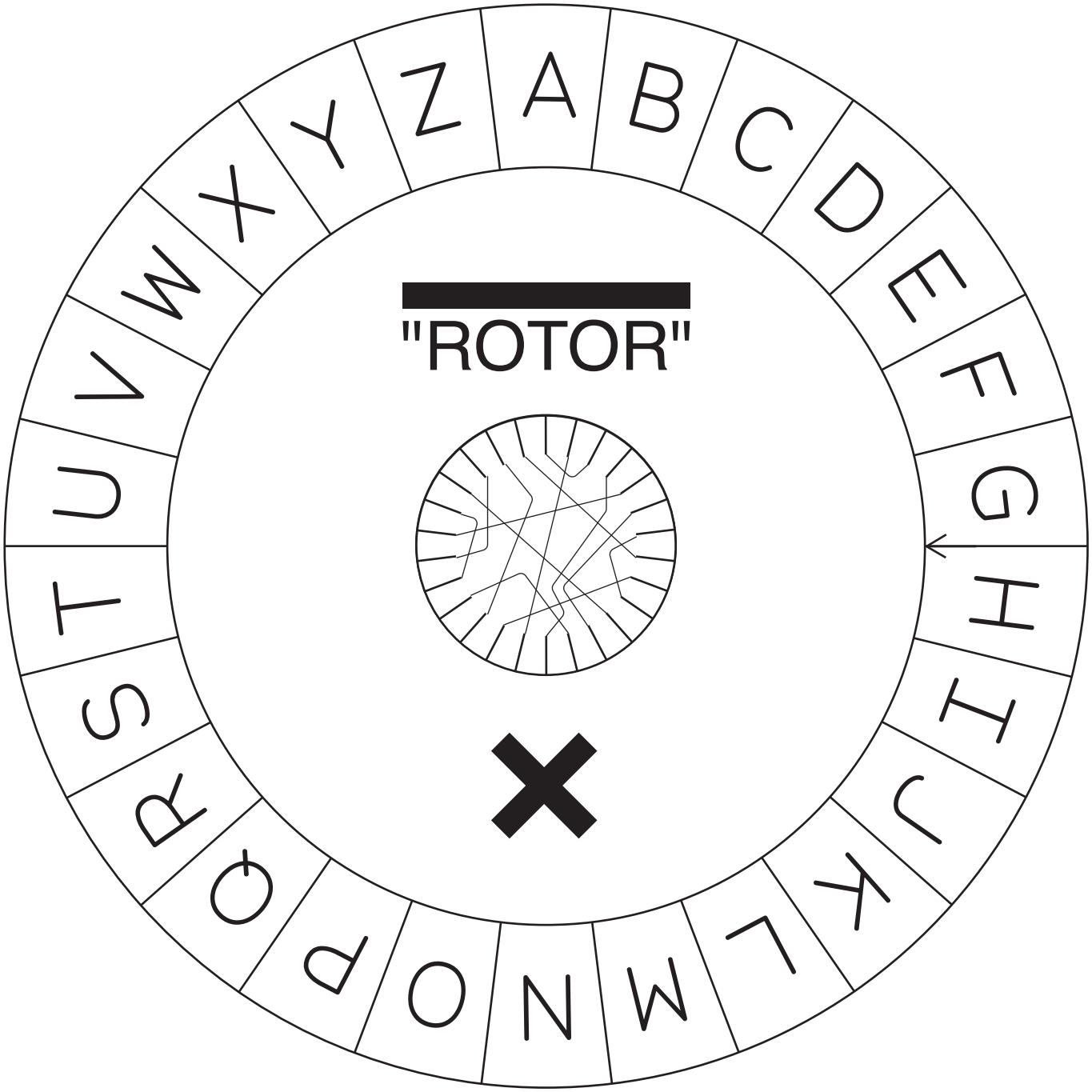
Vous savez que la séquence "RAPPORTMETEO" se cache quelque part dans la séquence de l'en-tête: "RFUOXLHRMDCFHPUC". Il s'agit de déterminer l'alignement correct de ces deux séquences de lettres l'une par rapport à l'autre.
Découpez les deux séquences de lettres dans les quadrillages et replacez "RAPPORTMETEO" en-dessous de "RFUOXLHRMDCFHPUC". Vous avez devant vous deux lignes horizontales de lettres, l'une au-dessus de l'autre. La ligne du haut est sensée coder celle du bas.
Vous devrez vous servir de la faille pour procéder à des éliminations: rappelez-vous, une lettre ne peut être codée par la même lettre.
Pour chaque possibilité d'alignement des deux séquences de lettres, vous devrez vérifier chaque "paire" verticale. Par conséquent, faites coulisser "RAPPORTMETEO" d'un cran vers la droite et répétez l'opération en faisant apparaître à chaque fois un nouvel alignement. Il suffit qu'une paire présente deux lettres identiques pour que l'alignement en question soit éliminé.
Relevez les positions qui conviennent. Vous devriez en avoir trouvé deux. Le champs des possibilités est désormais suffisamment réduit.

8) Parmi les positions qui s’offrent à vous, le but est de déterminer, entre les deux, laquelle correspond véritablement au réglage initial exact de la machine.
Maintenant, saisissez votre machine, choisissez n’importe quelle lettre et tournez le “rotor” jusqu'à ce qu’il vous indique le bon code (Ex : faisons l’hypothèse que la lettre A soit le code de la lettre F, vous devrez alors positionner le “rotor” de telle sorte que le A donne un F et inversement). Vous avez trouvé ? Parfait.

9) Vous voici en possession d’une machine opérationnelle. Maintenant que vous avez trouvé une partie du message, je vous propose de vous intéresser à son intégralité. Il vous suffit de décoder toutes les autres lettres en n'oubliant pas de tourner d'un cran à chaque fois. Bonne chance !

*** "AIDE"**
Pour vous assurer que vous avez bien compris : le code que vous auriez dû obtenir est "TTEBZGJJTIC".

ANNEXES pages suivante

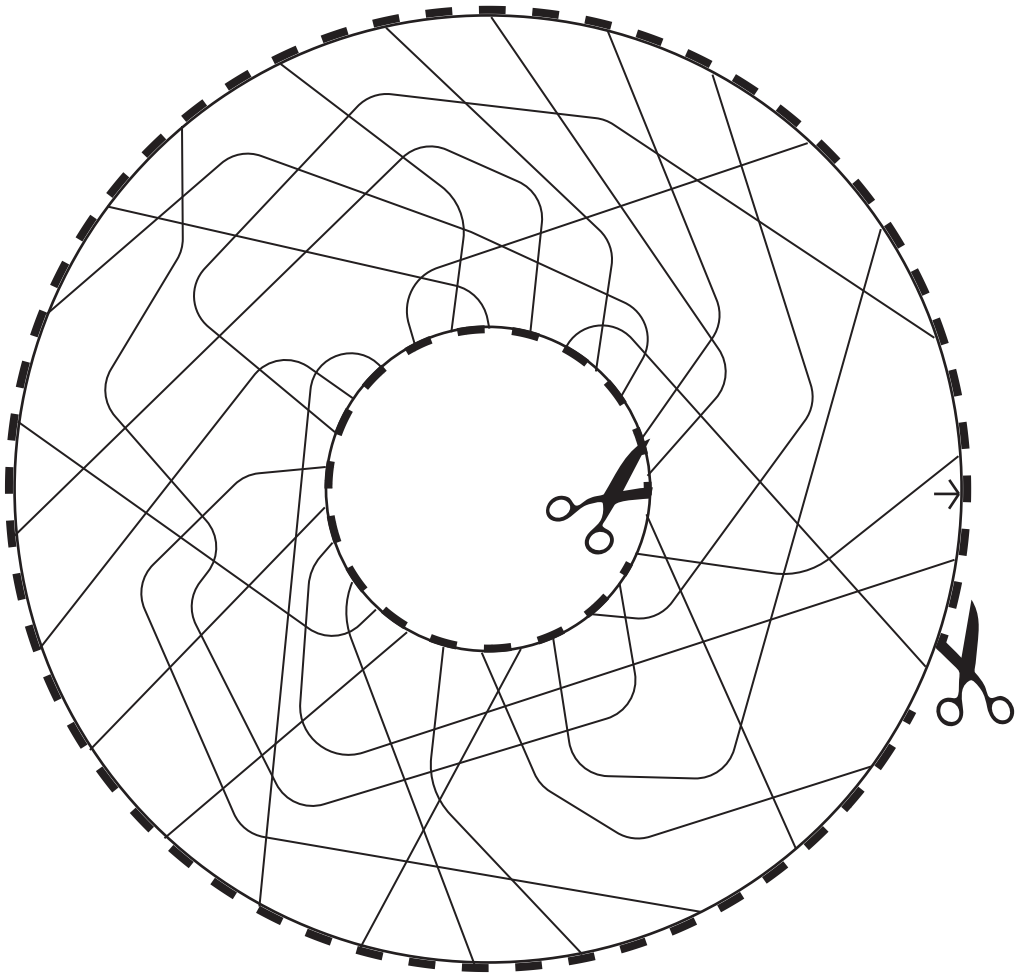


"LIKE OTHER ROTOR MACHINES, THE ENIGMA MACHINE IS A COMBINATION OF MECHANICAL AND ELECTRICAL SUBSYS-TEMS"

"DIE CHIFFRIERMASCHINE ENIGMA"

ENIGMA

R	U	O	X	L	H	R	M	D	C	F	H	P	U	C
R	A	P	P	O	R	T	M	E	T	E	O			



"ROTOR"