Laboratoire Mathématiques & Interactions
J.A. Dieudonné - UCA/CNRS - Nice
http://mathemarium.fr

Mathemarium
LJAD - UCA - CNRS

Cryptographie

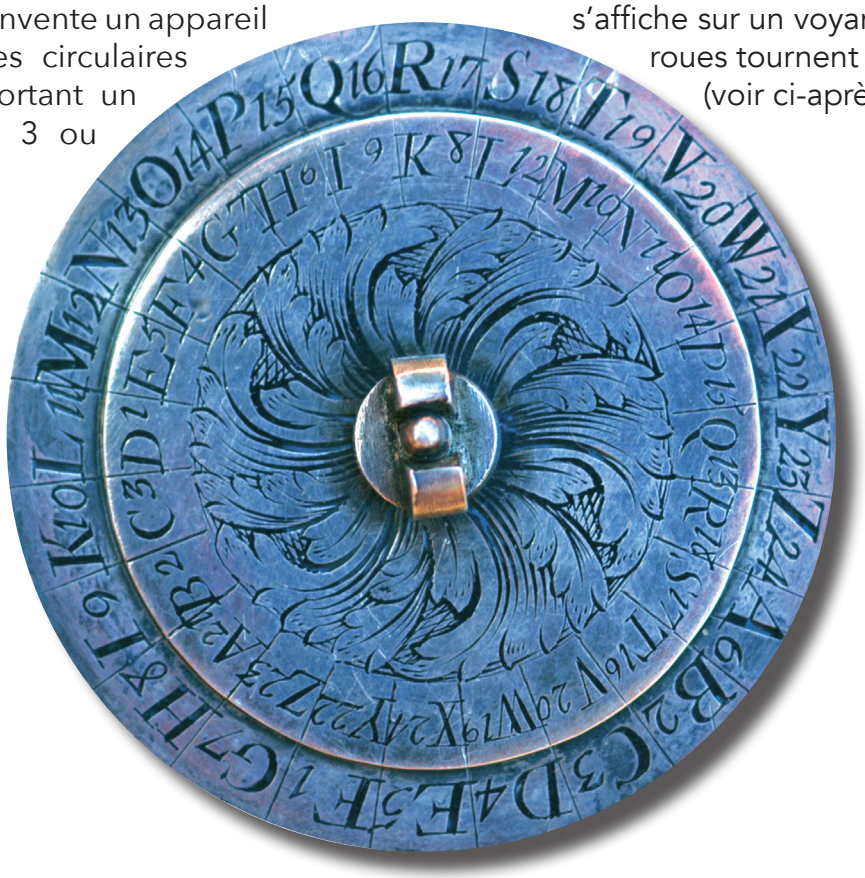
Cadran d'Alberti

Au XVe siècle, *Léon Battista Alberti* imagine un système de cryptage par substitution **polyalphabétique** :

la transformation d'une lettre en une autre n'est pas fixe comme dans le cryptage par translation (A->D), car la correspondance de transformation change au fur et à mesure du cryptage (ex : A->D, puis A->J, …).

Pour y arriver, Alberti invente un appareil formé de deux roues circulaires centrées, chacune portant un alphabet. Toutes les 3 ou 4 lettres cryptées, on tourne la roue centrale d'un cran, ce qui change les correspondances des lettres.

La machine **Enigma** reproduit exactement ce mécanisme de base, mais de façon plus complexe - on enchaîne en quelque sorte 3 ou 4 cadrans d'Alberti - et plus automatisées - on tape les lettres sur un clavier de machine à écrire, le résultat de la transformation de la lettre s'affiche sur un voyant lumineux, et les roues tournent automatiquement (voir ci-après).



cnrs INSMI
UNIVERSITÉ CÔTE D'AZUR

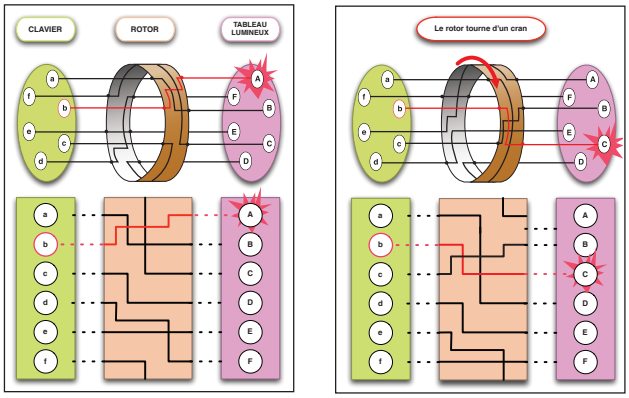
fête de la Science

ENIGMA

Développée par l'ingénieur Allemand Arthur Scherbius à partir de 1918, elle a été utilisée par les Allemands durant la seconde guerre mondiale pour protéger le contenu de leurs communications. Elle a été au coeur d'une bataille mathématique pour hacker le code et décrypter les messages.

Les Rotors au coeur du codage

PRINCIPE



- *On tape «b». Le courant passe dans le rotor. «A» s'allume.*
- *Le rotor tourne d'un cran.*
- *Si on retape «b». Maintenant, c'est la lettre «C» qui s'allume.*

FONCTIONNEMENT

- On appuie sur une touche.
- un lettre s'affiche, la lettre chiffrée.
- un mécanisme fait tourner le rotor de droite.

- Toutes les 26 frappes, le deuxieme rotor tourne d'une cran.
- Toutes les 676 frappes (26*26), le troisième rotor tourne d'un cran.

RAFFINEMENTS

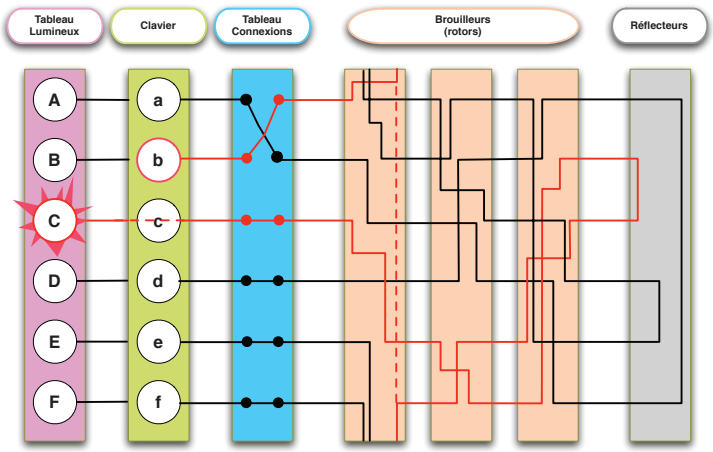
- TABLEAU DE CONNEXIONS : il permet de brouiller les pistes en reliant deux lettres du clavier entre elles.
- RÉFLECTEUR : c'est lui qui donne à la machine Enigma son «caractère involutif» (une involution est une opération qui est son propre inverse). Grâce à lui l'Enigma permet de coder et décoder les messages exactement de la même façon.
- DÉCALAGES des ROTORS : permet de décaler les lettres par rapport aux rotors.

10.586.916.764.424.000
combinaisons différentes

Le réglage de la machine fait toute sa puissance (clefs).
Dans une Enigma à 3 rotors on obtient :

- 26 x 26 x 26 = 17.576 combinaisons liées à l'orientation des chacun des trois brouilleurs (rotors)
- 6 combinaisons possibles liées à l'ordre dans lequel sont disposés les brouilleurs
- 100.391.791.500 branchements possibles sur le tableau de connexions.

soit au total 10.586.916.764.424.000 combinaisons différentes de crypter un texte.



Fabriquer sa machine de cryptage polyalphabétique

- Découper les cadrans en suivant les pointillés extérieur;
- Percer un trou au milieu de chaque cadran ;
- Assembler le cadran de base avec un cadran de cryptage au moyen d'un attache au centre.

Test
Utiliser le **cadran 2**, positionner le point noir du cadran de cryptage sur la lettre **L** du cadran de base (le n° de cadran et la position de départ du point noir est notre clef de cryptage : **2 - L**). Puis esayer de décoder le message suivant : JMNZFIN. Quel est le résultat ?