# Les pères de la cryptologie

## « Léon » Battista Alberti (18-2-1404 à Gènes 20-4-1472 à Rome)

par Daniel TANT

La Renaissance a produit en Italie plusieurs hommes universels, dont Alberti, un érudit qui se tourne vers les Ordres et la littérature.

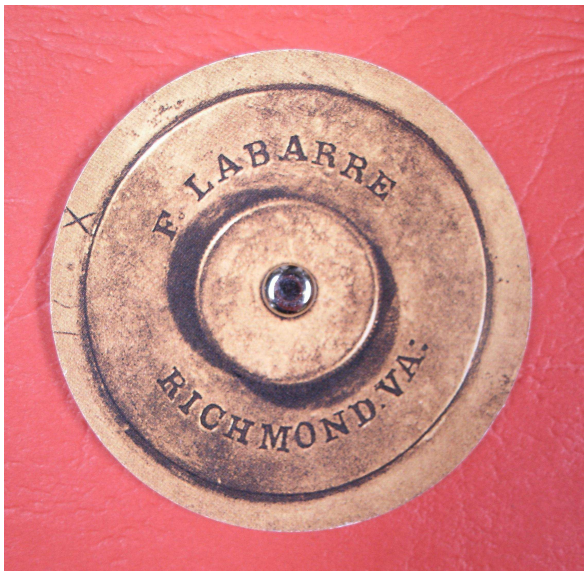
A 56 ans, dans son livre *« De Componendis Cyphris »* il propose un système avec deux alphabets pour casser la fréquence utilisée par les cryptanalystes en fonction des lettres les plus fréquentes dans une langue. A la fin de l'ouvrage il décrit son invention : le cadran chiffrant appelé depuis disque d'Alberti.

Il est donc le père de la substitution polyalphabétique qui a donné naissance bien plus tard aux principes des machines à rotors.

De plus, il crée le principe du surchiffrement à partir de son disque.


*Le disque alphabétique inventé par Alberti a été utilisé très longtemps. Ci-dessus, la copie du disque utilisé par le gouvernement et l'armée confédérée pendant la guerre de sécession. Il ne reste actuellement que 5 disques originaux.*

*ci-contre à gauche : une version métallique de ce disque est en vente dans le commerce. Il est fourni avec la pochette de velours pour son transport.*





*Sous Louis XIV, Nicolas Bion crée un ensemble composé d'un disque fixe et de quatre disques amovibles, dont voici une réplique approximative, car l'original est orné de fioritures.*

*Avec le positionnement présent entre les deux disques, le mot cryptographie devient : NZFXBWOZHXPQM.*

*ci-dessus :*

*fabriqué en 1984, ce disque provient d'une tenue de « super-héros ». La couronne extérieure correspond au texte en clair.*

*En prenant, par exemple, le chiffre 13 comme clé de départ (voir la fenêtre en haut du disque), le texte « J'arrive demain » devient :*

*3XEEQ8I9IDXQO.*