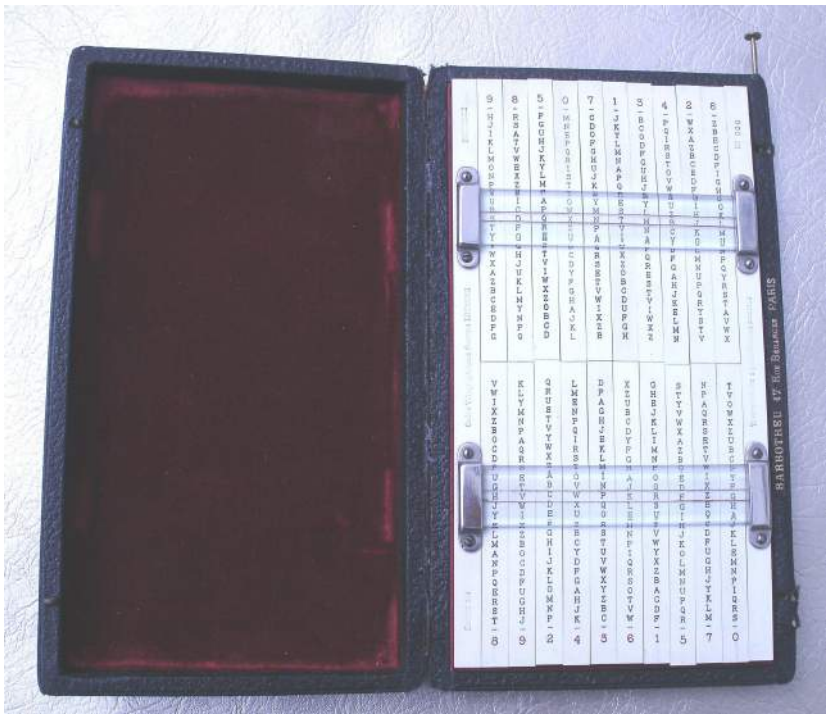
Le transpositeur à permutations secrètes

Par Daniel TANT

Au début du XXème siècle la société de Georges Lugagne à Marseille fabrique des systèmes d'encodage destinés aux entreprises civiles, car la concurrence est rude et il importe que les différents employés et représentants d'une société puissent communiquer en toute sécurité avec leur entreprise.

Georges Lugagne a donc créé un système fiable et astucieux pour l'époque qui se présente sous la forme d'une petite machine composée de touches en ivoire, ce qui permet de cryptographier en toutes les langues utilisant l'alphabet romain.



Le Transpositeur à permutations secrètes dans son étui de transport.

L'appareil se présente sous la forme d'une tablette plate, légère et présentée dans un étui pouvant tenir dans une poche. Il fonctionne sans électricité ni utilisation d'un code lourd et encombrant. Autonome, il est conçu pour casser la fréquence des lettres bien connue des décrypteurs, et offre 13 168 189 440 000 possibilités et cependant il peut être volé, perdu ou oublié sans risque de compromission concernant les messages échangés.

Son utilisation et sa compréhension sont à la portée de tous et la formation des opérateurs est très rapide.

Il est composé de 20 réglettes en bois étuvé résistant aux variations de température et en cas de casse, il est possible d'échanger une réglette seule ce qui rend cet appareil très économique.

Hélas le transpositeur à permutations secrètes n’a pas atteint la perfection car son rendement est très faible et ne convient pas à un échange élevé de messages codés.

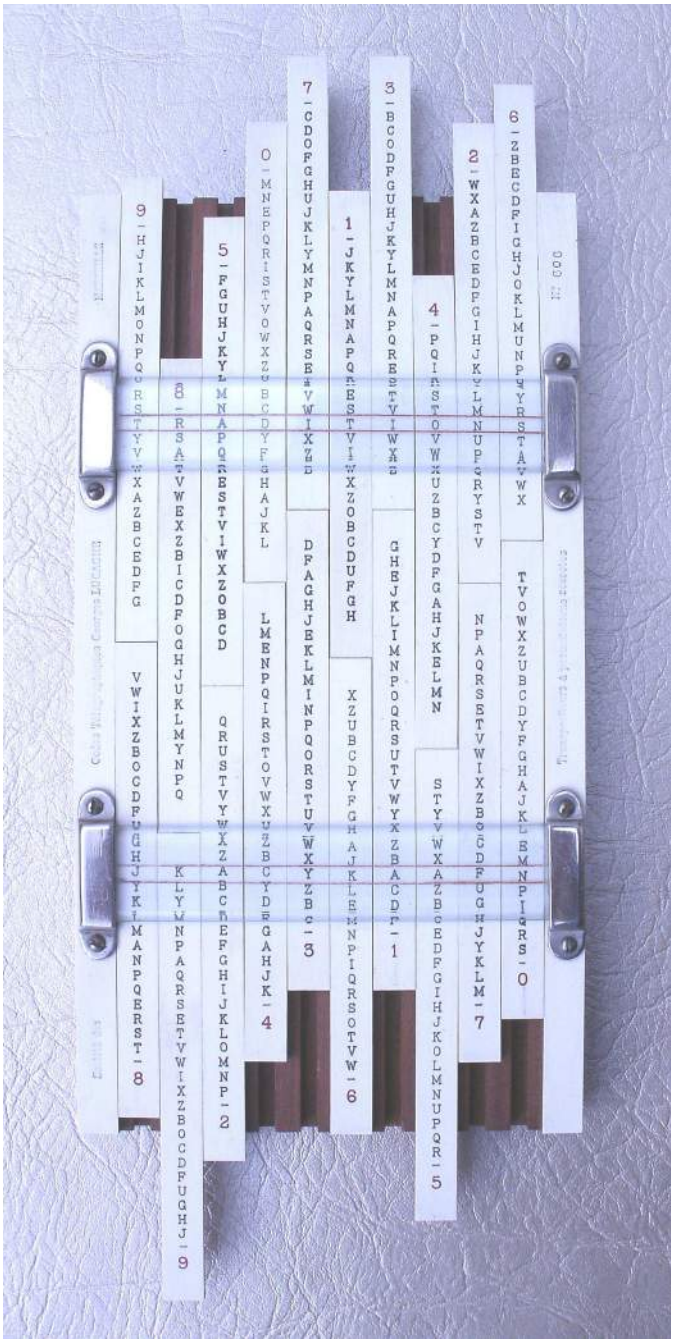
Le support est entaillé de 20 rainures dans lesquelles glissent 20 réglettes mobiles, déplaçables, couvertes de nacre sur lesquelles sont gravées sur chacune un alphabet dans l’ordre aléatoire plus le tiret.

10 réglettes numérotées en haut de 0 à 9 sont affectées au langage clair et 10 autres numérotées en bas de 0 à 9 pour le langage crypté. Elles se placent donc tête-bêche en deux séries de 10.

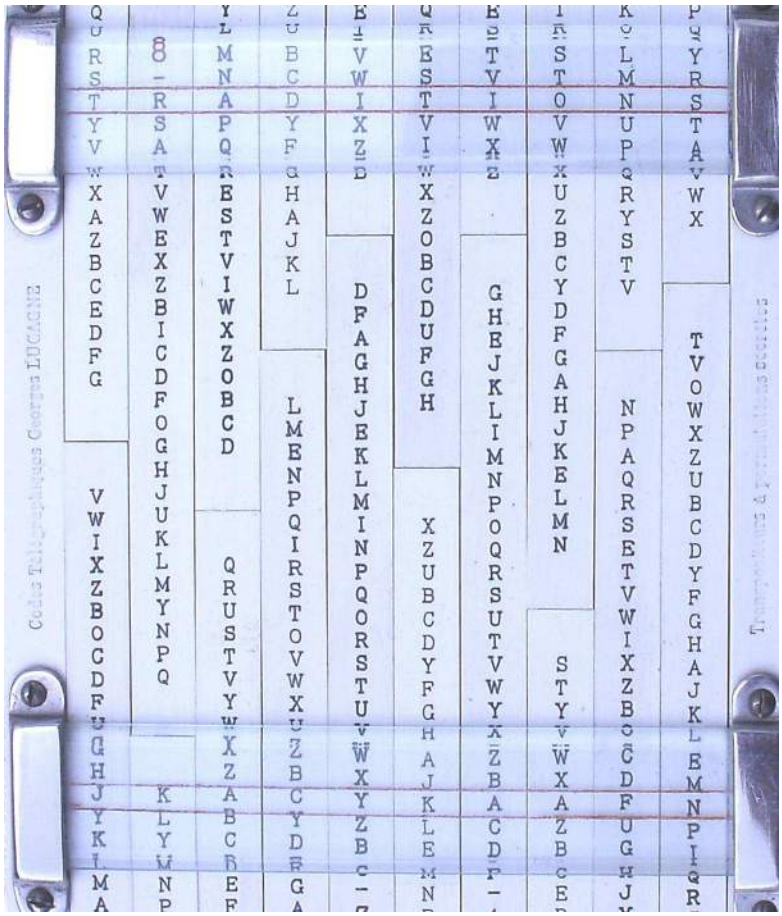
Les réglettes sont interchangeables et des réglettes transversales transparentes laissent apparaître à travers deux guides, les lettres en clair et en chiffré.

Le problème est de ne pas introduire dans le message la clé de départ, à savoir l’ordre numérique des réglettes.

Le dispositif a été breveté sous le N 461217 en 1913. Une version mécanisée, se présentant sous forme de calculette munie de 20 disques à engrenage à été breveté en 1922 sous le N°537446 mais il ne semble pas qu’elle ai été fabriquée.



ci-contre à droite : le transpositeur en cours d’utilisation. La clé donnant l’ordre des réglettes se donne de gauche à droite, réglettes clair puis réglettes du texte codé, ce qui donne : 98507134268924361570.



A travers la réglette transparente du haut apparaît le mot en clair : traditions.

A travers la réglette transparente du bas apparaît le mot codé : jkacykaafn.

Le procédé est simple et universel. Mais il est particulièrement lent pour coder une page entière.

ARCSI - Association des Réservistes du Chiffre et de la Sécurité de l'Information
Association régie par la loi de 1901 - N° SIRET : 511 069 569 00016
Tous droits de propriété intellectuelle réservés à l'ARCSI, association loi 1901, selon les règles du droit français