



Association des Réservistes du Chiffre et de la Sécurité de l'Information

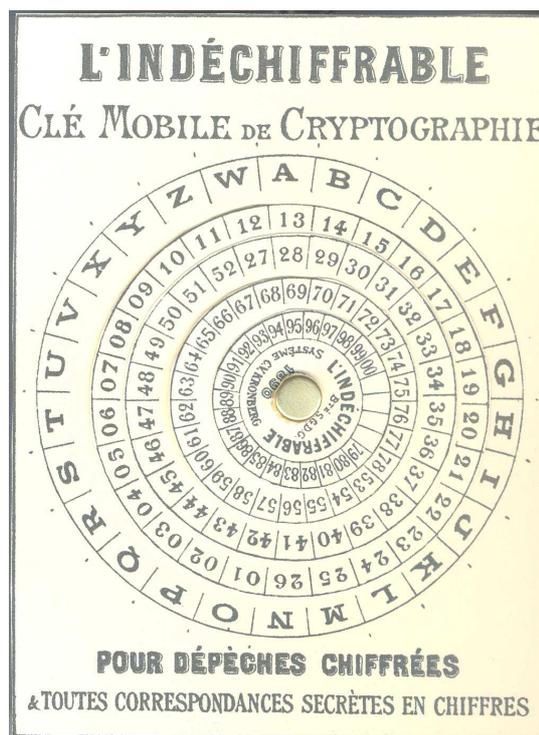
L'indéchiffrable par Daniel TANT

Depuis que l'écriture existe, les procédés de chiffrement n'ont cessé de se perfectionner car les « cabinets noirs » ont inventé des méthodes de codage qui résisteraient aux décrypteurs ennemis.

En voici un publié en novembre 1890 par la Revue universelle des inventions nouvelles, breveté S.G.D.G. en 1890 par C. Kronberg et qui améliore le disque d'Alberti.

Il est composé de quatre disques mobiles et un disque fixe, attachés au centre par une attache parisienne.

La carte servant de support mesure 10,5 centimètres de haut sur 8 centimètres de large. Chaque disque est divisé en 26 cases. Le disque extérieur, imprimé sur la carte, correspond au texte en clair et contient les vingt six lettres de l'alphabet.



Les disques mobiles contiennent également 26 rayons entre lesquels sont écrits 99 nombres de 2 chiffres.

Dans le cas présent il suffit de communiquer d'abord la clé de départ à partir de la lettre A, suivie du texte crypté, soit dans le cas présent, pour coder le mot « cryptographie » :

13 28 69 95 - 30 04 66 02 06 57 19 45 95 43 20 36 99

Cette invention propose donc 450 000 combinaisons pour la clé de départ.

Il est à noter que, pour une raison inconnue, sur le disque fixe extérieur, la lettre W se situe entre le Z et le A.