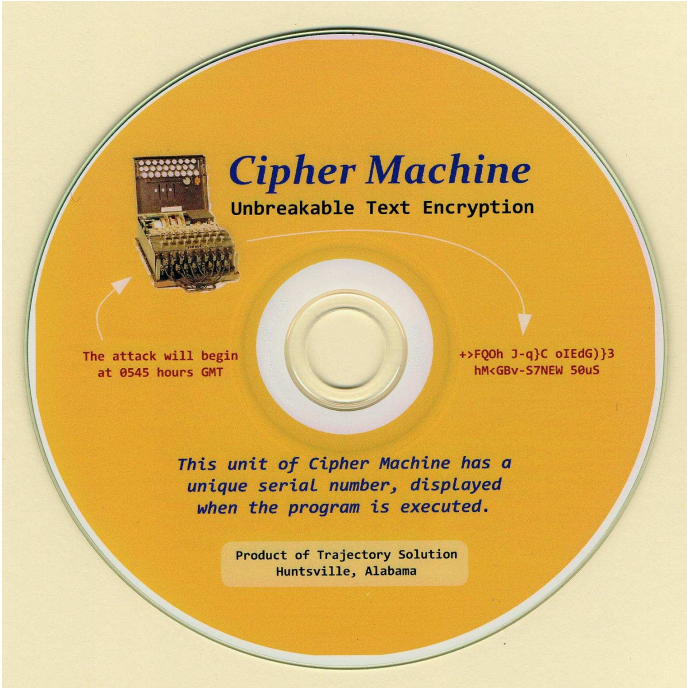
Un logiciel autrefois incassable

Par Daniel TANT

Aujourd'hui il n'est plus nécessaire de posséder de coûteuses machines à rotors. Voici un logiciel vendu librement dans le commerce et qui tient son originalité dans le nombre de clés possibles.



Il est capital que le chiffreur et le déchiffreur possèdent la même clé de départ et que celle ci puisse résister aux ordinateurs de décryptement comme ceux de la N.S.A. Un jour ou l'autre le message sera « cassé » et le jeu consiste à retarder le plus possible cette échéance.

Sur un disque à un seul alphabet, pour casser le message il faut essayer chacune des 26 lettres, soit 26 essais.

Sur un appareil à deux rotors la tentative portera sur 26 X 26 lettres, soit 676 essais.

Avec ce logiciel, la clé de départ comporte 8 signes, soit les 26 lettres de l'alphabet minuscules ou majuscules, et tous les signes figurant sur le clavier.

Il est possible, par exemple de choisir :)/ ?)-« µR ou b-']$&vX

La clé distingue les lettres minuscules et les lettres majuscules.

Effectivement, le message ne risque pas d'être cassé immédiatement, mais les performances techniques de ce logiciel sont dépassées.

Le fabricant est installé aux U.S.A.