Date: Dimanche 30 avril 2006 à 04:25:00
Sujet: 7 Cryptographie

La cryptographie de Porta (substitutions polyalphabétiques)

Le physicien italien Della Porta (1540-1615) fut l'inventeur du premier système littéral à double clé, c'est à dire le premier chiffre pour lequel on change d'alphabet à chaque lettre.

Porta emploie 11 alphabets différents, qu'il désigne, comme on le voit dans la figure ci- contre par AB, CD, EF etc. Si on veut écrire avec un de ces alphabets, on choisit pour représenter les lettres du texte clair, celles qui leur font face. Par exemple, si l'on cryptographiait avec l'alphabet A ou B, on représente a par n et vice-versa n par a. Porta recommande d'écrire chaque lettre avec un alphabet différent. De plus, pour ne pas obliger les correspondants à prendre les onze alphabets à la suite, il propose de n'en adopter que quatre, cinq ou six et de convenir d'un mot clé dont les lettres indiqueront les alphabets qu'il faudra successivement choisir. Bien sûr, il est déconseillé d'utiliser un alphabet régulier comme indiqué ci-dessus (a b c d e ...). Il vaut mieux utiliser des alphabets composé des 26 lettres réparties aléatoirement. Della Porta le recommandait déjà lui-même dans son traité : « De furtivis litterarum notis, vulgo de ziferis; Naples 1563 ».

A B a b c d e f g h i l m n o p q r s t v x y z C
D a b c d e f g h i l m z n o p q r s t v x y E
F a b c d e f g h i l m y z n o p q r s t v x G
H a b c d e f g h i l m x y z n o p q r s t v I
L a b c d e f g h i l m v x y z n o p q r s t M
N a b c d e f g h i l m t v x y z n o p q r s O
P a b c d e f g h i l m s t v x y z n o p q r Q
R a b c d e f g h i l m r s t v x y z n o p q S
T a b c d e f g h i l m q r s t v x y z n o p V
X a b c d e f g h i l m p q r s t v x y z n o Y
Z a b c d e f g h i l m o p q r s t v x y z n

Publication de Tout sur l'informatique - Programmation C#, Sécurité, Divx, P2P:
http://www.zmaster.fr

URL de cette publication
http://www.zmaster.fr/modules.php?name=News&file=article&sid=181