

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.

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

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>