

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 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 ».

Porta 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

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