

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 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		E
z n o p q r s t v x y			
F	a b c d e f g h i l m		G
y z n o p q r s t v x			
H	a b c d e f g h i l m		I
x y z n o p q r s t v			
L	a b c d e f g h i l m		M
v x y z n o p q r s t			
N	a b c d e f g h i l m		O
t v x y z n o p q r s			
P	a b c d e f g h i l m		Q
s t v x y z n o p q r			
R	a b c d e f g h i l m		S
r s t v x y z n o p q			
T	a b c d e f g h i l m		V
q r s t v x y z n o p			
X	a b c d e f g h i l m		Y
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#,
Scurit, Divx, P2P:
<http://www.zmaster.fr>

URL de cette publication

<http://www.zmaster.fr/modules.php?name=News&file=article&sid=181>