

Date: Lundi 04 octobre 2004 à 22:49:46
Sujet: 7 Cryptographie

Le carre de Polybe

Polybe est un célébre historien grec et conseiller militaire Romain. Il invente vers 150 av JC un procédé de cryptage tenant dans un carré de 5 de coté.

Donc il n'y a que 25 lettres alors que l'alphabet en compte 26 , et
oui le "w" a été enlevé (c'est la
deuxiémé lettre la moins utilisée en francais
) . Le cryptage est assez simple il suffit de choisir une lettre par
exemple "h" et de le remplacer par le numero de la
rangée; suivi du numero de la colonne donc $h=23$. Ensuite
Polybe avait choisit de ranger les chiffres par groupe de 3 pour
rendre plus difficile la cryptanalyse et les chances que l'ennemi
casse le code.

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=16>