

# « Cryptage » n'existe pas en français

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 Juin 2007

<http://www.bortzmeyer.org/cryptage-n-existe-pas.html>

---

On voit souvent le terme de « **cryptage** » apparaître dans les articles ou messages au sujet de la cryptographie. Mais ce terme n'existe pas en français et, pire, représente une erreur de compréhension.

Revenons sur la cryptographie. Un message (le « texte en clair ») qu'on veut rendre illisible à un espion est transformé par un algorithme paramétré par une clé (une suite de nombres). La connaissance de l'algorithme **et** de la clé est normalement nécessaire pour opérer la transformation inverse et donc pour lire le message.

Mais certaines techniques, collectivement regroupées sous le nom de **cryptanalyse** permettent parfois de retrouver le message même sans connaître la clé. C'est ainsi que sont nés les termes :

- **chiffrer** = « coder » le texte en clair, grâce à la clé, pour produire un texte chiffré, illisible,
  - **déchiffrer** = « décoder » (retrouver le texte en clair) quand on connaît le « code » (le fonctionnement normal),
  - **décrypter** = « décoder » quand on ne connaît pas le « code » (grâce à la cryptanalyse).
- « crypter » voudrait donc dire « coder » sans clé, n'importe comment, sans aucune possibilité de « décoder » après opération.

Wikipédia, à juste titre, note que « le chiffrement est parfois appelé à tort cryptage » mais a la gentillesse de rediriger vers l'article Chiffrement lorsqu'on cherche Cryptage.

Le seul dictionnaire de français utilisable en ligne que je connaisse (à part bien sûr le Wiktionnaire), le Trésor de la Langue Française ne connaît, lui, ni cryptage, ni chiffrement ! Le Dictionnaire en ligne de l'Académie Française, quoique difficilement utilisable (il faut apparemment un logiciel spécifique, non libre, pour le lire), me permettra de presque terminer cet article sur un argument d'autorité : il ne connaît que chiffrement et pas cryptage.

Le livre de référence sur la cryptanalyse est bien sûr « *The code breakers* » <<http://www.bortzmeyer.org/codebreakers.html>> » de David Kahn, mais dont je déconseille la traduction française, très boguée. Sinon, le plus ancien texte public que j'ai trouvé sur ce faux terme de « crypter » date de 1999 <<http://groups.google.com/group/fr.misc.cryptologie/msg/308271497c0b03ec>>.