« Cryptage » n'existe pas en français

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 juin 2007. Dernière mise à jour le 8 janvier 2019

https://www.bortzmeyer.org/cryptage-n-existe-pas.html

On voit souvent le terme de « **cryptage** » apparaitre 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 connaitre 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.

J'emprunte à hyper <https://mastodon.gougere.fr/@hyper> un bon exemple : « les Alliés ont **décrypté** Enigma mais mon navigateur Web a **déchiffré** la connexion HTTPS ».

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.

Il y a peu de dictionnaires de français utilisable en ligne (le premier étant bien sûr le Wiktionnaire). Le Trésor de la Langue Française ne connait, lui, ni cryptage, ni chiffrement. Ceci dit, c'est un peu normal, me fait remarquer fatfrog, il s'arrête délibérement en 1960 et n'a pas été modifié depuis 1994 (« Avertissement : la rédaction du TLF est terminée depuis 1994 et la plupart des contributeurs ont quitté le

laboratoire. Il n[Caractère Unicode non montré [1]]a pas vocation à être mis à jour. Cette ressource, qui ne fait pas l[Caractère Unicode non montré]objet d[Caractère Unicode non montré]une veille lexicographique, est donc close "en l[Caractère Unicode non montré]état". Il est donc tout à fait naturel que les définitions qui s[Caractère Unicode non montré]y trouvent ne rendent pas compte des évolutions de la société. ») Le Larousse cite cryptage <http://www.larousse.fr/dictionnaires/francais/cryptage/20841?q=cryptage#20720> sans commentaire et sans rien y comprendre. Le Dictionnaire de l'Académie Française, accessible en ligne via le CNRTL <http://www.cnrtl.fr/definition/academie9>, me permettra de presque terminer cet article sur un argument d'autorité : il ne connait que chiffrement et pas cryptage (« Cette forme est introuvable ! », neuvième édition). Depuis, ladite Académie a produit une note <http://academie-francaise.fr/crypter> (repérée par Laurent Blum) qui montre une incompréhension complète de la question. « Crypter » est une erreur technique, pas de français !

Le livre de référence sur la cryptanalyse est bien sûr « "*The code breakers*" <https://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>. Beaucoup plus récemment, en 2011, il y a eu un bon article d'explication avec schémas chez Ryfe <http://www.ryfe.fr/2011/08/les-mots-crypter-et-cryptage-n%E2%80%99existent-pas/>. Et il y a bien sûr l'excellent chiffrer.info <https://chiffrer.info/>.

1. Car trop difficile à faire afficher par LaTeX