RFC 7801 : GOST R 34.12-2015: Block Cipher "Kuznyechik"

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 mars 2016

Date de publication du RFC : Mars 2016

https://www.bortzmeyer.org/7801.html

Encore un algorithme de cryptographie venu de l'Est, avec cette spécification sous forme de RFC d'un algorithme GOST, connu sous le petit nom de « Kuznyechik » (dans la transcription anglo-saxonne), et, plus formellement, sous celui de GOST R 34.12-2015. C'est un algorithme de chiffrement symétrique par blocs.

Comme d'autres algorithmes de cryptographie normalisés par GOST, Kuznyechik a été développé en partie par le secteur public (Service des communications spéciales et d'information du Service fédéral de protection de la Fédération de Russie) et par le secteur privé (InfoTeCS <http://www.infotecs.ru/>). Le décret n° 749 du 19 juin 2015, pris par l'Agence fédérale pour la régulation technique et la métrologie en a fait un algorithme russe officiel. C'est donc apparemment un concurrent d'AES.

Les sections 3 et 4 du RFC décrivent l'algorithme en détail. Pour les connaisseurs en cryptographie seulement, d'autant plus que le format actuel (c'est en cours de révision) des RFC n'est pas idéal pour décrire des mathématiques, il vaut mieux utiliser la version en anglais de la norme russe <http://tc26.ru/en/standard/gost/GOST_R_34_12_2015_ENG.pdf>. Des vecteurs de test figurent en section 5.

Merci à André Sintzoff, qui sait utiliser Canard, canard, va.