RFC 5830 : GOST 28147-89 encryption, decryption and MAC algorithms

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 mars 2010

Date de publication du RFC : Mars 2010

https://www.bortzmeyer.org/5830.html

Les algorithmes de signature et de chiffrement GOST sont des normes russes de cryptographie. Leur utilisation est obligatoire en Russie pour les services publics. GOST est un algorithme purement local, qui n'avait été décrit qu'en russe et qui n'avait donc jamais suscité d'intérêt à l'étranger. Sauf erreur, ce RFC 5830 [1] (et son compagnon, le RFC 5832, sur l'algorithme de signature) sont les premières descriptions « officielles » de GOST en anglais. Les RFC précédents comme le RFC 4490 ou le RFC 4491 ne portaient que sur l'usage de GOST. (Depuis, une nouvelle version de l'algorithme est sortie, spécifié dans le RFC 8891.)

GOST 28147-89, décrit dans notre RFC, est la norme russe de chiffrement et déchiffrement symétrique (GOST R 34.10-2001, décrit dans le RFC 5832, étant l'algorithme de signature).

La section 4 donne le cadre général de l'algorithme. On note que, s'il dépend de tables de substitution, aucune n'est définie dans la norme (on peut en trouver dans le RFC 4357). Classiquement, il existe plusieurs modes de chiffrement comme ECB (décrit en détail en section 5) ou CFB (section 7). GOST 28147-89 permet également de générer un MAC (section 8).

Ces deux RFC sur GOST ont suscité des débats agités à l'IETF, notamment face à la possibilité de leur incorporation dans DNSSEC. Les critiques portaient sur l'insuffisance de la description dans le RFC (bien des points sont laissés dans l'ombre <http://www.ietf.org/mail-archive/web/ietf/current/msg60221.html> et il semble difficile de mettre en œuvre GOST uniquement en lisant le RFC), sur le peu d'analyse de sécurité sérieuse faite sur GOST, et sur les vraies motivations du gouvernement russe pour insister à imposer un algorithme local (une des hypothèses étant, comme toujours avec les gouvernements fermés, qu'il y a une porte dérobée dans l'algorithme).

Ce RFC a été remplacé depuis par le RFC 8891, qui décrit une version plus récente de l'algorithme.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5830.txt