

## NIST szuka nowej funkcji skrótu

<http://ipsec.pl/nist-szuka-nowej-funkcji-skrotu.html>

W związku ze stopniowym wycofywaniem z użycia funkcji skrótu SHA-1 amerykańska organizacja standardyzacyjna NIST (National Institute for Standard and Technology) ogłosiła plany rozpisania konkursu na nową rodzinę funkcji skrótu, które mają zastąpić SHA-1. Konkurs będzie miał przebieg podobny do tego w jakim kilka lat temu wyłoniono szyfr AES - zainteresowane firmy i instytucje mogą zgłaszać swoje propozycje standardu, które będą rozpatrywane przez komisje NIST oraz poddane publicznej recenzji.

Nowa funkcja ma generować skróty o długościach od 224 do 512 bitów (obecnie SHA-1 daje 160 bitów) i być w stanie pracować na blokach o długości do  $2^64$  bitów. *Algorytm musibyć tak że pozbawiony "pulapek" licencyjnych*  
*ahref = "http://www.csrc.nist.gov/pki/HashWorkshop/timeline.html" > wstepnego kalendarza konkursu </a > ostatecznego wyłonienia zwycięzcymamyćmiejsce w 2012 roku.*

W marcu ubiegłego roku NIST [ja href="http://www.csrc.nist.gov/pki/HashWorkshop/NIST](http://www.csrc.nist.gov/pki/HashWorkshop/NIST)

Źródło: [ja href="http://www.csrc.nist.gov/pki/HashWorkshop/index.html"](http://www.csrc.nist.gov/pki/HashWorkshop/index.html) i "NIST's Plan for New Cryptographic Hash Functions" [i/a](#)