

2009 yılı hash (özet) fonksiyonları yılı olacak (3)

Bir yıllık bir çalışma sonucunda ortaya çıkan 51 SHA-3 özet fonksiyonu adayı, ABD Ulusal Standardlar ve Teknoloji Enstitüsü (NIST) tarafından düzenlenen ve Belçika'nın Leuven kentinde 23-28

Şubat tarihlerinden yapılacak olan Birinci SHA-3 Adayları Konferansı'nda tasarımcılar tarafından sunulacak. Bu konferansta bir kısım aday algoritmalar çakışma bulunmuş olması nedeniyle kırılmış sayılacak, bir kısmı ise tam kırılmasa bile, herhalde tasarımcılar tarafından yeteri kadar kuvvetli görülmediği için geri çekilecek. Bütün bu çalışmalar ve heyecan ortaya güzel bir sonuç çıkarmak için yapıyor. Bu konferansta olmazsa bile, ikinci veya üçüncü SHA-3 konferansında adayların sayısı 5e veya 6ya kadar inmiş olacak. AES algoritmasının seçimine çok benzeyen bu süreç sonucunda, SHA-3 algoritmasına kavuşmuş olacağız.

SHA-3 algoritmasına ihtiyacımız var. SHA-1 algoritmasını NIST'in getirdiği ku-



**ÇETİN KAYA
KOÇ**

ral gereği 2010'dan sonra kullanmayacağız. SHA-2 aile kullanılabilir ama aynı prensiplere dayandığı için tedbirli olmakta fayda var. SHA-3 adaylarına dikkatli bakıldığında, dünyasına dört bir yanında tasarlanmış bu

algoritmaların özgünlüklerini hemen farkediyorsunuz: <http://tinyurl.com/62532t>. Bazıları eski fikirleri farklı yapılar içinde devam ettiriyor ancak bazıları ise yepyeni fikirler içeriyor. Tasarımcılar içinde, kriptografi biliminin ağır siklet oyuncularını var, örneğin, Dan Bernstein, Lars Knudsen, Joan Daemen (AES tasarımcısı) ve Ron Rivest. Ben ortaya çıkacak SHA-3 algoritmasının, Rijndael (AES) gibi başarılı olacağına inanıyorum.

Söylenecik birkaç söz daha var. Listeye baktığınızda dört tane Türkçe tasarımcı ismi göze çarpıyor. Bu da onur verici bir gelişme tabii. AES adayları tasarımcıları içinde Türkiye kökenli araştırmacılar yoktu ama SHA-3 içinde var. Yani SHA-3 çorbasında Türkiye tuzu da var!

koc@cryptocode.net