

2009 yılı hash (Özet) fonksiyonları yılı olacak (1)

2006 yılı Nisan ve Mayıs aylarında yazdığım yazılarda anlattığım gibi ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yayınlanan Federal Bilgi İşleme Standartları (FIPS), hem ABD içindeki

kurumlar hem de uluslararası kurumlar tarafından kabul edilmekte ve doğal olarak uluslararası standartlar haline gelmekte. Bu standartlardan önemli bir grup, hash (özet) fonksiyonları. Şu anda NIST tarafından onaylı 5 hash fonksiyonu var: SHA-1, SHA-224, SHA-256, SHA-384, ve SHA-512. Bunlardan son dördüne SHA-2 ailesi deniyor ve hash değeri uzunluğu isimleri içinde belirtilmiş (örneğin, SHA-224, 224 bitlik hash değerleri üretiyor). SHA-1 en eski olanı ve uzunluğu ise 160 bit. Prensipten olarak bir hash fonksiyonunun güvenliği onun bit uzunluğunun yarısı değerinde. Bu durumda, SHA-1 güvenliği 80-bit olarak addediliyor. Ancak, Ağustos 2005'te kriptografi araştırmacıları, SHA-1 algoritmasında bir zayıflık keşfettiler. Aslında SHA-1 güvenliğinin 63 bit olduğu gibi bir önerme var önümüzde. Şimdiye kadar hiç kimse,



**ÇETİN KAYA
KOÇ**

SHA-1 algoritmasını örnekler üzerinde kırmış değil. Ancak bu şüpheler, NIST araştırmacılarını harekete geçirdi. 15 Mart 2006'da bir genelge yayınlayarak, SHA-1 algoritmasının 2010'dan itibaren kullanılmaması

gerektiğini söylediler. Bu genelge, özellikle e-imza ve zaman damgası gibi güvenlikleri çok önemli olan uygulamalar için geçerli. Bu genelge, Türkiye e-imza uygulamalarını da içeriyor çünkü bizde SHA-1 kullanıyoruz. NIST'in genelgesi 2010'dan sonra SHA-2 ailesinin kullanılması yönünde öneride bulunuyor.

Ancak burada şöyle önemli bir problem var: SHA-2 ailesi ve SHA-1 prensip olarak aynı metotlar üzerine kurulu. Akademik dünyanın kriptografi uzmanları ise, SHA-2 ailesine geçişin iyi fikir olmadığını düşünüyor, çünkü doğal olarak SHA-1 türü zayıflıkları barındırıyorlar. Peki ne olacak, SHA-1 yerine SHA-2 kullanamayacaksak (veya o zamana kadar SHA-2 ailesinde de zayıflıklar keşfedilmişse!), ne kullanacağız? Cevap: SHA-3 kullanacağız. SHA-3 ile ilgili bilgiler bir sonraki yazımızda. koc@cryptocode.net