

## 2009 yılı hash (özet) fonksiyonları yılı olacak (2)

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Kasım 2007'de yayınladığı bir genelge ile yeni bir özet fonksiyonu seçmek için uluslararası bir yarışma açtığını duyurdu ve bilim adamı ve

mühendislere kendi SHA-3 özet fonksiyonlarını tasarlayıp sunma çağrısı yaptı. Bu genelgede, NIST, SHA-0, MD4 ve MD5 algoritmalarının çakışma (collision) nedeniyle artık kullanılamayacağını, SHA-0 algoritmasında çakışma bulmak için gereken denemelerin sayısının gerekenden az olduğu, ve SHA-1 üzerinde Kasım 2007 itibariyle henüz bir çakışma bulunmadığını belirtti. Gerçekten de hatta bugüne kadar (Ocak 2009) henüz SHA-1 üzerinde bir çakışma bulunmuş değil, ancak konuyu yakından takip eden bir kişi olarak bunun çok uzakta olmadığını (belki 2009 yılı içinde!) söylemem lazım. Örneğin, Arjen Lenstra, yüzlerce Sony Playstation donanımı ile şu an denemeler yapmakta ve ayrıca farklı donanımlar üzerinde SHA-1 çakışması arayan başkaları da var. Diğer yandan, NIST, şu an SHA-2 ailesinden şüphe etmek için bir ne-



**ÇETİN KAYA  
KOÇ**

denimiz yok diyor, ancak, bir zayıflık bulunması elektronik imza protokollerini katastrofik bir şekilde etkileyecektir diye çok doğru ve uzak görüşlü bir değerlendirme yapıyor. Elimizde bir SHA-3 olması çok faydalı

olacaktır, diyor.

AES algoritmasının uluslararası bir yarışma ile seçilmiş olması ve AES üzerindeki oluşan güvenin gittikçe artması da SHA-3 algoritmasını böyle bir metotla seçmenin doğru olacağını düşündürüyor. Sonuç olarak, NIST, genelgesinde SHA-3 algoritmasının kısa bir sürede seçilip ortaya konmasının iyi bir tedbir olacağını belirtti. Tamamiyle AES seçimi metotlarına sadık kalarak (dünya çapında yarışma ve hiç bir patent hakkı iddia edilmemesi şartları ile), SHA-3 yarışmasını Kasım 2007'de başlattı ve 31 Ekim 2009'e kadar yarışmacılara süre verdi.

Bu tarih geçmişte kaldı. Yarışmacılar, toplam 64 tane algoritmayı iletiler ve bunlardan 13 tanesi kurallara uymadıkları için yarışma dışı kaldı, geriye kalan 51 tane NIST tarafından yayınlandı: <http://tinyurl.com/62532t>  
**koc@cryptocode.net**