# Özet (Hash) fonksiyonları üzerine

ÇETİN KAYA KOÇ

Sayısal imza fonksiyonları bilindiği gibi açık anahtarlı şifreleme tekniğine dayanır.

Kriptografik özet fonksiyonları bilgi güvenliği mekanizmalarının bir çoğunda karşımıza çıkar ve genellikle veri bütünlüğünü sağlamak ve doğrulamak amacı ile kullanılır. Önemli uygulamalardan birisi sayısal imzadır. Sayısal imza fonksiyonları bilindiği gibi açık anahtarlı şifreleme tekniğine dayanır. Kullanıcı kendisine ait ve gizli (private) anahtarı ile veriyi şifreler ve bu şifrenin doğruluğunu herhangi bir kişi kullanıcının açık (public) anahtarı ile teyit eder.

En çok kullanılan ve uluslararası açık anahtarlı şifreleme metodu RSA algoritması dahil olmak üzere bilinen bütün açık anahtarlı şifreleme algoritmaları sayılar, sonlu alanlar ve grup teorilerine dayanırlar. Böyle matematiksel algoritmalar ne yazık ki "çarpımsal saldırı" (multiplicative attack) denilen saldırı türlerine açıktırlar. Bu saldırıyı uygulayan rakip bir kişi, eski imzalardan yeni imzalar türetebilir. İşte bu yüzden sayısal imzalar hiç bir zaman veri üzerine direkt olarak uygulanmaz; verinin özeti üzerine uygulanır çünkü özet değerlerine çarpımsal saldırı yapmak imkansıza yakın bir derecede zordur.

Buraya kadar herşey yolunda gözükse de, aslında pek öyle değil. Çünkü özet fonksiyonlarının da başka problemleri var. En büyük problem "çakışma" (collision) problemi. Bu iki farklı verinin aynı özete sahip olması demek. Bunu istemiyoruz çünkü imzalarda eşdeğer olur. Böyle verileri bulmanın zorluğu ise özet fonksiyonunun ürettiği özet değerinin yarı uzunluğu ile alakalı. Mesela MD5 özet fonksiyonu 128 bitlik özet değerler üretir, yani çakışma bulmak için yapılacak denemelerin sayısı 264 kadar olmalıdır. Bu kadar deneme yapmak artık günümüzde mümkün. Bunu 1 günde gerçekleştirmek için gerekli yatırım yüzbin dolarlar mertebesinde. İşte bu yüzden MD5 artık güvenli değil ve bir uluslararası standart olarak kabul edilmiyor.

MD5 özet fonksiyonunun yerine SHA-1 denilen ve özet uzunluğu 160 bit, yani güvenlik derecesi 280 olan bir fonksiyon geçti. Artık uzun bir süre güvendeyiz derken, 2005 Şubat ve Ağustos aylarında araştırmacılar SHA-1 algoritmasına bir saldırı açıkladılar ve SHA-1 algoritmasının güvenirliği konusunda şüpheler belirdi. Bu araştırmanın detaylarını ve ne anlama geldiğini, sabrınıza sığınarak, bir sonraki yazımda açıklayacağım. Peki bütün bunlar bizi ilgilendiriyor mu? Evet, ilgilendiriyor. Çünkü SHA-1 algoritması, Türkiye'nin e-imza uygulamasının bir parçası. Türkiye'de özel ve kamu sertifika merkezlerinin kök sertifikaları ve verdikleri tüm sertifikalar SHA-1 kullanıyor.

*koc@cryptocode.net*