

# E-İMZADA SHA-1 ÖZETLEME ALGORİTMASININ KULLANIMI\*

Çağdaş Çalık, Meltem Sönmez Turan, Zaliha Yüce

ODTÜ Uygulamalı Matematik Enstitüsü  
Kriptografi Bölümü  
{e110870,msonmez,e120371}@metu.edu.tr

**ÖZET :** Özetleme fonksiyonları, mesaj bütünlüğü kontrolü ve kimlik doğrulanması mekanizmalarının önemli bir parçasıdır. Bu sebeple, özetleme fonksiyonlarında bulunabilecek zayıflıklar elektronik imza (e-imza) uygulamalarının güvenliğini tehlikeye düşürebilir. Nitekim, son zamanlarda e-imzada kullanılan SHA-1 özetleme algoritmasına yönelik ciddi saldırılar yapılmıştır. Bu çalışmada, özetleme algoritmaları kısaca tanıtıldıktan sonra e-imza kullanımında SHA özetleme fonksiyon ailesinin durumu verilmiştir.

**ANAHTAR KELİMELER:** Elektronik İmza, Özetleme Fonksiyonları , SHA-1

## USE OF SHA-1 HASH ALGORITHM IN DIGITAL SIGNATURES

**ABSTRACT :** Hash functions have an important role in systems where message integrity and authentication is used. Therefore, weaknesses found in hash functions algorithms also reduce the security of digital signature applications. As a matter of fact, some attacks about the hash function SHA-1 which is used in digital signatures have been announced. In this study, after a brief summary of hash functions, the status of SHA hash function family is given.

**KEYWORDS :** Digital Signatures, Hash Functions, SHA-1

### Giriş

Özetleme fonksiyonları verilen herhangi bir uzunluktaki metnin sabit uzunluktaki özetini oluşturur. Bu fonksiyonlar tek yönlü oldukları için veri bütünlüğü ve kimlik doğrulanması ile ilgili uygulamalarda temel yapıtaşı haline gelmiştir. SHA-1 [1], MD5 [2], RIPEMD [3] en çok kullanılan özetleme fonksiyonlarıdır. SHA ve MD5, https ve SSL gibi internet trafiğinde, PGP ve S/MIME gibi e-posta şifreleme uygulamalarında, VPN gibi özel bilgisayar ağlarında, SSH ve SFTP gibi güvenli uzaktan ulaşım uygulamalarında ve kimlik belirleme gibi birçok uygulamada kullanılmaktadır.

E-imza uygulamalarında hız büyük önem taşıdığı için önerilen algoritmaların çoğunda tüm mesaj yerine mesajın özeti imzalanır. Tebliğde referans olarak verilen ETSI TS 102 176-1 standardına göre e-imza uygulamalarında Türkiye’de SHA-1 algoritması kullanılması önerilmektedir. Ancak 2005 yılında, SHA-1 özetleme fonksiyonu ile ilgili zayıflıklar yayınlanmıştır [4]. Bu çalışmada, e-imza uygulamalarında da standart olarak verilen SHA-1 algoritma-

sının zayıflıkları ve alınması gereken önlemler belirtilmiştir.

### Özetleme Fonksiyonları ve Özellikleri

Bir özet fonksiyonu,  $H$ , verinin sayısal karşılığını  $M$ 'yi kullanarak, sabit uzunluğa sahip mesajın özetini,  $h=H(M)$ , oluşturur. İlk olarak uzun mesajı,  $m_1, m_2, \dots, m_n$  olmak üzere eşit uzunlukta bloklara ayrılır. Gerektiği durumlarda son blok belirli bir fonksiyon kullanarak blok uzunluğuna tamamlanır.  $H_0$  başlangıç vektörü ve  $f$  sıkıştırma fonksiyonu olmak üzere,  $H_i=f(H_{i-1},M_i)$  değerleri hesaplanır. Sıkıştırma fonksiyonunun son kez kullanıldığında elde edilen çıktı, mesajın özeti olarak kullanılır.  $H$  fonksiyonunun iç yapısı açıktır ve gizli anahtar içermez, dolayısıyla şifreleme yapmak için kullanılmazlar.

Özetleme fonksiyonunun güvenli olarak kullanabilmesi için aranan bazı özellikler vardır. Bunlardan birincisi, özetleme fonksiyonunun tek yönlülük özelliğidir, yani özetini kullanarak özeti alınan mesaja ulaşmak kolay olmamalıdır (pre-image resistance). Mesaj kümesi özet kümesinden çok daha büyük olduğu için veri kaybı olur, dolayısıyla geri dönülemezler. Mesaj özetinden algoritmayı geriye doğru çalıştırıp  $2^n$ den

\* Bu çalışma 1056126 numaralı 1007 TÜBİTAK Kamu Projesi tarafından desteklenmemiştir.

daha az işlemde mesaj elde edilebildiği takdirde özet fonksiyonunun tek yönlülük özelliği kırılmış olur.

İkinci özellik, verilen herhangi bir mesaj M için, M'den farklı ve aynı özete sahip başka bir mesaj bulunması zor olmalıdır (2nd pre-image resistance). Özetleyecek olursak, kriptografik özetleme fonksiyonlarının sağlaması gereken temel özellikler aşağıda belirtilmiştir.

- Özetlenecek mesaj (girdi) herhangi bir boyutta olabilir.
- Mesaj özeti (çıkıtı) sabit bir uzunluktadır.
- Verilen herhangi bir mesaj için özeti hesaplanması kolay olmalıdır.
- $H(x)$  tek yönlü olmalıdır.
- $H(x)$  çakışmalara dayanıklı olmalıdır.

## SHA Özetleme Fonksiyon Ailesi

SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması), Amerika'nın ulusal güvenlik kurumu olan NSA (National Security Agency) tarafından tasarlanmış ve ilk olarak 1993 yılında FIPS PUB 180 standardında yayınlanmıştır. Sıkıştırma fonksiyonundaki küçük bir değişiklikle 2 yıl sonra tekrar NSA tarafından SHA-1 adında FIPS 180-1 de yayınlanmıştır.

SHA-1, uzunluğu en fazla  $2^{64}$  bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında, ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar. SHA-1 çalışma prensibi olarak R. Rivest tarafından tasarlanan MD5 özet fonksiyonuna benzer ve iteratif bir yapısı vardır. Her iterasyonda bir sıkıştırma fonksiyonu kullanır. Bu fonksiyon, mesajın 512 bitlik bloğunu alır ve 16 bitlik kelimelere ( $m_0, m_1, \dots, m_{15}$ ) çevirir. Daha sonra bu kelimeler,  $m_i = (m_{i-3} + m_{i-8} + m_{i-14} + m_{i-16}) \lll 1$  fonksiyonu kullanılarak 2560 bite genişletilir ve her biri 20 matematiksel fonksiyon içeren 4 tur çalıştırılır ve 160 bitlik mesajın özeti elde edilir.

## SHA1'in Kırılması

Mesaj özetleri aynı olan iki farklı mesaj bulunması durumuna çakışma adı verilir. N elemanlı bir popülasyonda, bir çakışma gerçekleşebilmesi için ortalamada  $\sqrt{n}$  tane rasgele örnekleme yapılması beklenmektedir. Dolayısıyla,  $2^{n/2}$  lik karmaşıklaktan daha az işlemle çakışma bulan bir algoritma özet fonksiyonunu kırılmış sayılır. Özetleme fonksiyonlarının çakışmalara karşı dayanıklı olmaları gerekmektedir. Elektronik imzalarda çakışmalar kullanılarak yapılan ataklarda birbirine zıt anlam içeren ancak mesaj özetleri aynı olan iki mesaj bulunur. İmza atan kişi imzayı kabul etmeyerek, zıt anlamlı mesajı imzaladığını öne sürebilir. Bu tür atakların önlenmesi için çakışmaların bulunması zor olmalıdır. 160 bit çıkıtı üreten bir özetleme

fonksiyonu çakışmalara karşı 80 bitlik güvenlik sağlamalıdır.

SHA özetleme algoritmalarına yapılan ilk atak ile SHA-0 algoritmasında beklenenden daha kısa bir sürede çakışmalar bulunmuştur [5]. Benzer atak SHA-1'e uygulandığında her hangi bir zayıflık tespit edilememiştir. Daha sonradan SHA-0'a yapılan ataklarla birlikte özetleme fonksiyonunun güvenilirliği 39 bite kadar düşmüştür [6]. 2005 yılında, SHA-1 fonksiyonunda çakışmaları  $2^{63}$  işlemde bulan bir atak geliştirilmiştir [4]. İşlem sayısı fazla olmasına rağmen, pratikte bu işlem gücüne sahip bilgisayar ağları bulunmaktadır.

Özetleme fonksiyonlarına yapılan çakışma atakları mesajın belirlenmesi kadar riskli olmasa da birçok güvenlik açığı oluşturur ve genel kaniya göre, bir özet fonksiyonu çakışma ataklarına dayanıklı değilse, kısa zamanda özet fonksiyonunun bütün kullanım alanlarında da risk ortaya çıkar.

SHA özet fonksiyon ailesinde çıkıtı uzunluğu daha uzun olan ve küçük farklar içeren ve SHA-2 ailesi olarak adlandırılan dört farklı algoritma (SHA-224, SHA-256, SHA-384 ve SHA-512) bulunur. Bu algoritmaların özellikleri Tablo 1'de özetlenmiştir. SHA-0 ve SHA-1 için geliştirilmiş ataklar SHA-2 versiyonları için herhangi bir zayıflık belirtmemiştir. Ancak SHA-2 algoritmasının yapısı SHA-1'e benzemediğinden bu algoritmalarında yakın zamanda kırılma ihtimallerine karşı araştırmacılar yeni algoritma tasarlamaya karar vermişlerdir.

	Mesaj Uzunluğu	Blok Uzunluğu	Mesaj Özeti	Güvenlik
SHA1	$< 2^{64}$	512	160	80
SHA256	$< 2^{64}$	512	256	128
SHA384	$< 2^{128}$	1024	384	192
SHA512	$< 2^{128}$	1024	512	256

Tablo 1 SHA fonksiyonlarının karşılaştırılması

## Sonuç

Günümüzde oldukça yaygın olarak kullanılan SHA-1 algoritmasının kırılmasıyla birlikte özetleme fonksiyonları tekrar önem kazanmıştır. 31 Ekim – 1 Kasım 2005 tarihlerinde ABD Standartlar Enstitüsü (NIST) tarafından yapılan bir konferansta özetleme fonksiyonlarının durumu tartışılmış [7] ve SHA-2'nin yapısal özelliklerinin SHA-1'e benzemesinden dolayı ilerde kırılabilirliğinin düşünülmesi NIST'i yeni bir özetleme fonksiyonu bulma çabasına itmiştir. Ancak özetleme fonksiyonlarının hangi kriterlere göre değerlendirilip kabul edilebileceği konusundaki bilgi eksikliğinin tamamlanması, seçilen fonksiyonun yaygınlaştırılması, yazılım ve donanımın adapte olmasının da yıllar alacağı bilinmektedir.

15 Mart 2006 tarihinde NIST tarafından yapılan açıklamaya göre federal birimler e-imza, zaman damgası ve çakışmaya karşı dayanıklılık gerektiren bütün uygulamalarda SHA-1 kullanımının en kısa zamanda durdurulmasını ve 2010 yılı itibariyle mutlaka SHA-2 ailesinin kullanımına geçilmesinin gerekliliğini belirtmiştir [8].

Koç [9] tarafından da vurgulandığı gibi, Türkiye'de verilen tüm sertifikalarda kullanılan SHA-1 özetleme algoritmasından en kısa zamanda SHA2 ailesine geçiş yapılmalıdır ve aynı zamanda yazılımlar ve donanımla değişikliklere olanak sağlayacak şekilde tasarlanmalıdır.

## Kaynaklar

- [1] "Secure Hash Standard", FIPS PUB 180-1, 1995
- [2] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, 1992
- [3] Dobbertin H., Bosselaers A., Preneel B., "RIPEMD-160: A Strengthened Version of RIPEMD", Fast Software Encryption, 71-82, 1996
- [4] X. Wang, Y. L. Yin, and H. Yu. "Finding Collisions in the Full SHA-1" Crypto, 2005
- [5] Chabaud F., Joux A., "Differential Collisions in SHA-0", Advances in Cryptology, 1998
- [6] X. Wang, H. Yu, Y. L. Yin, "Efficient Collision Search Attacks on SHA-0", Crypto, 2005
- [7] Noll, L. J., "SHA1 Cryptographic Hash Update", Systems Experts, <http://www.systemexperts.com/tutors/CryptographicHashUpdate.pdf>
- [8] NIST, [http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/NIST\\_Policy\\_on\\_HashFunctions.htm](http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/NIST_Policy_on_HashFunctions.htm)
- [9] Koç, Ç. K. "Özet (Hash) fonksiyonları üzerine", BT Haber, Sayı:567, 2006