**HASH (ÖZETLEME) Fonksiyonları**

Alınan bir verinin boyutundan bağımsız olarak sabit uzunlukta ve alınan veriye özel üretilen çıktıdır. Yani aynı veriye her zaman aynı çıktıyı üretilir.

Örneğin; Hash fonksiyonlarından biri olan MD5 ile ***“****Oturarak ayakta alkışlıyorum****”*** girdisinin çıktısı her zaman *“03b1e500069350efdfb7391f174008f1”* şeklinde olacaktır. Bu değer sadece bizim kullandığımız girdiye oluşacaktır. Aynı zamanda *“Oturarak ayakta alkışlıyorum, çünkü buna değersin”* şeklinde girdimizin boyutunu arttırırsak yine aynı uzunlukta ve yine o girdiye özel farklı *“7a71d4e4cfc86896c419c42698bd9fe9”* çıktısı oluşacaktır.

İki farklı girdinin aynı çıktıyı üretmesi (buna Collision=Çatışma denir) o Hash fonksiyonunu kırıldığının göstergesidir. SHA-1 ve MD5 kırılan Hash fonksiyonlarına örnek olarak verilebilir.

Hash fonksiyonları;

* veritabanında şifrelerin turulmasında
* büyük verilede değişiklik olup olmadığının kontrolünde
* e-posta şifreleme uygulamaları
* güvenli uzaktan erişim uygulamaları
* internetten güvenli şekilde veri indirme işlemleri gibi alanda kullanılır.

Bazı Hash fonksiyonlarından bahsedersek;

1. **MD5 (Message Digest 5 = Mesaj Özetleme 5)**

Boyutu fark etmeksizin algoritmaya girişi yapılan bir girdinin çıkışı olarak 128-bit uzunluğunda 32 karakterli 16'lık sayı sisteminde bir dizi elde edilir. *(Yukarıdaki örneği incelersek oradaki girdilerin boyutunun 32 karakterli olduğunu görürüz.)*

Tek yönlü çalışır. Yani şifreleme yapılır, ancak şifre çözüm işlemi yapılamaz. Bu durum parola kullanılan sistemlerde dezavantaj olarak değerlendirilir.

Örneğin; Üye olduğunuz bir sitede parolanız MD5 hash fonksiyonundan geçirilerek veritabanında tutuluyor. Siz parolanızı unuttuğunuzda ve sitede buna dair bir işlem yaptığınızda site size eski parolanızı değil yeni parola gönderecektir.

1. **SHA1 (Secure Hashing Algorithm = Güvenli Özetleme Algoritması)**

MD5 ve SHA1 arasındaki temel fark oluşturdukları özetlerdeki boyut farkıdır.

SHA1’ de girişi yapılan bir girdinin çıkışı olarak 160-bit uzunluğunda 40 karakterli 16'lık sayı sisteminde bir dizi elde edilir.

***“****Oturarak ayakta alkışlıyorum****”*** girdisi 40 karakterden oluşan *“717ff8f9ae35f7df358ebd8f34d3fad04847380f” çıktısını oluşturur.*

Teknik özellikler dışında SHA1 den bahsedecek olursak; Kriptanalistlerin 2005'te yaptığı bir saldırıyla SHA1'in yeterince güvenli olmadığını ispatladılar. Bu yüzden 2010' dan beri SHA1 yerine daha güvenli olan SHA2  kullanımı tercih ediliyor. Microsoft, Google, Apple ve Mozilla SSL Sertifikalarından 2017 itibarıyla SHA1 desteğini çekeceklerini açıkladılar. Daha sonra ise Google SHA1’ e çakışma saldırısı yaptıklarını ve iki farklı PDF dosyasından aynı SHA1 özet çıktıyı aldıklarını ispatlayarak SHA1 in kırıldığını duyurdular.

Ayrıca SHA1 Git, Mercurial ve Monotone gibi dağıtık revizyon kontrol sistemlerinde revizyonların belirlenmesinde ve veri bozulmalarının veya müdahalelerinin algılanmasında kullanılmaktadır.

1. **SHA-2 Ailesi**

Şimdi gelelim MD5 ve SHA1 fonksiyonlarından daha güvenli olmasına rağmen hızlı bir geçiş yapılamayan SHA-2 ailesinin hikayesine… ☺

Bu durumun nedeni; Windows XP, SP2 veya daha üst sürümü çalıştıran sistemlerin SHA2 için desteklenmemiş olmasıydı.

Bu süreci hızlandırmak için Google Chrome ekibi, web tarayıcısının 2014'ün sonlarından 2015'in başlarına kadar bir süre boyunca SHA1'e bağımlı TLS sertifikalarını kademeli olarak reddetmek için bir plan yaptıklarını açıkladı. Benzer şekilde Microsoft, Internet Explorer ve Edge'in kamuya açık SHA1 imzalı TLS sertifikaları Şubat 2017'den itibaren onaylamayacağını açıkladı. Böyleye SHA2’ ye geçiş hızlandırılmaya başladı.

SHA2 ailesi dememizden de anlaşılacağı gibi SHA2 alt gruplara sahiptir.

Alt gruplar SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.SHA-256 ve SHA-512 basamak uzunluklarına (bit cinsinden) göre isimlendirilmiş hash fonksiyonlarıdır.

Biz sadece SHA256, SHA384, ve SHA512 algoritmalarından kısaca bahsedeceğiz.

1. **SHA256**

Algoritma sonucunda 256-bit uzunluğunda 64 karakterli 16'lık sayı sisteminde bir dizi elde edilir.

***“****Oturarak ayakta alkışlıyorum****”*** girdisi 64 karakterden oluşan *“e1eb1591864e7aaeb9292f5315cfe7366a8ba8b508dabd1fb3a31d1fbb633334” çıktısını oluşturur.*

Ayrıca SHA256; Debian yazılım paketleridoğrulama sürecinde, Bitcoin kripto para birimi işlemlerinde doğrulama yapmak, para iletimlerini kanıtlamak veya hisseleri hesaplamak için kullanır.

1. **SHA384**

Algoritma sonucunda 384-bit uzunluğunda 96 karakterli 16’lık sayı sisteminde şifreli metin üretilir.

***“****Oturarak ayakta alkışlıyorum****”*** girdisi 96 karakterden oluşan *“35c65398b33426d9f5d1e90c3648085963c796ac9656ada2d0ff9001f1607363cbbd36a215742d1c78b3027b4195e996” çıktısını oluşturur.*

1. **SHA512**

Algoritma sonucunda 512-bit uzunluğunda 128 karakterli 16’lık sayı sisteminde şifreli metin üretilir.

***“****Oturarak ayakta alkışlıyorum****”*** girdisi 128 karakterden oluşan *“94a529b16f747ed0a743f95e73dbd8360f0aa1e27d46556e428a7986838f83985b858a3ad476719b73f79719618f5b28b8ae72a72bc7e8ba171518e4db255899” çıktısını oluşturur.*