Hash Fonksiyonları ve Dijital İmzalar Nedir?

Çalışma Kağıdı

Hash fonksiyonları, rastgele uzunluktaki veriyi sabit uzunlukta bir çıktıya (hash değeri veya özet) dönüştüren algoritmalar iken, dijital imzalar bu hash değerini kullanarak verinin kaynağını ve bütünlüğünü kriptografik olarak doğrular.

Sorular

1. Aşağıdakilerden hangisi hash fonksiyonlarının temel özelliklerinden biri DEĞİLDİR?

A) Tek yönlü olması (geri döndürülemez)
B) Aynı girdi için her zaman aynı çıktıyı üretmesi
C) Farklı girdiler için farklı çıktılar üretme olasılığının yüksek olması (çarpışma direnci)
D) Çıktıdan girdiyi kolayca elde edilebilmesi

2. Dijital imzanın doğrulanmasında hangi anahtar kullanılır?

A) Özel Anahtar
B) Açık Anahtar
C) Simetrik Anahtar
D) Her iki anahtar da aynı anda

3. Hash fonksiyonlarının 'çarpışma direnci' ne anlama gelir?

A) Farklı girdilerin aynı hash değerini üretme olasılığının düşük olması
B) Aynı girdinin farklı hash değerleri üretebilmesi
C) Hash değerinin kolayca tahmin edilebilmesi
D) Hash fonksiyonunun çok hızlı çalışması

4. Bir dosyanın bütünlüğünü doğrulamak için hash fonksiyonları nasıl kullanılır?

5. Dijital imza, bir belgenin kimliğini nasıl doğrular?

6. Tanımla: Hash Fonksiyonu Nedir?

7. Tanımla: Hash Değeri (Özet) Nedir?

8. Tanımla: Dijital İmza Nedir?

Cevap Anahtarı

1. D) Çıktıdan girdiyi kolayca elde edilebilmesi — Hash fonksiyonları tek yönlüdür, yani çıktıdan girdiyi kolayca elde etmek mümkün değildir. Bu, güvenliklerinin temelini oluşturur.

2. B) Açık Anahtar — Dijital imzayı doğrulamak için göndericinin açık anahtarı kullanılır. Özel anahtar ise imza oluşturmak için kullanılır.

3. A) Farklı girdilerin aynı hash değerini üretme olasılığının düşük olması — Çarpışma direnci, iki farklı girdinin aynı hash değerini üretme olasılığının matematiksel olarak çok düşük olmasıdır. Bu, hash fonksiyonunun güvenilirliği için önemlidir.

4. Gönderici, orijinal dosyaya bir hash fonksiyonu uygular ve bir hash değeri (özet) üretir.,Bu hash değeri, dosya ile birlikte alıcıya gönderilir.,Alıcı, aldığı dosyaya aynı hash fonksiyonunu uygular ve kendi hash değerini hesaplar.,Alıcının hesapladığı hash değeri ile göndericiden gelen hash değeri karşılaştırılır.,Eğer iki değer eşleşirse, dosyanın aktarım sırasında değiştirilmediği doğrulanır.

5. Gönderici, belgenin hash değerini hesaplar.,Gönderici, bu hash değerini kendi özel anahtarını kullanarak şifreler. Bu şifrelenmiş hash, dijital imzadır.,Orijinal belge ve dijital imza alıcıya gönderilir.,Alıcı, imzayı göndericinin açık anahtarını kullanarak deşifre eder ve orijinal hash değerini elde eder.,Alıcı, aldığı belgenin hash değerini kendisi hesaplar.,Deşifre edilmiş hash ile yeniden hesaplanan hash karşılaştırılır. Eşleşirse, imza geçerlidir ve belge göndericiden gelmiştir.

6. Rastgele uzunluktaki girdiyi sabit uzunlukta bir çıktıya (hash değeri) dönüştüren tek yönlü algoritma.

7. Hash fonksiyonunun çıktısı olan, verinin benzersiz bir parmak izi gibi davranan sabit uzunluktaki değer.

8. Verinin bütünlüğünü ve kaynağını doğrulamak için kullanılan, özel anahtar ile şifrelenmiş hash değeridir.