Blokzincir 101

Prof.Dr. Ali Hakan IŞIK
Res.Assist. Durmuş Gülbahar

2.Hafta

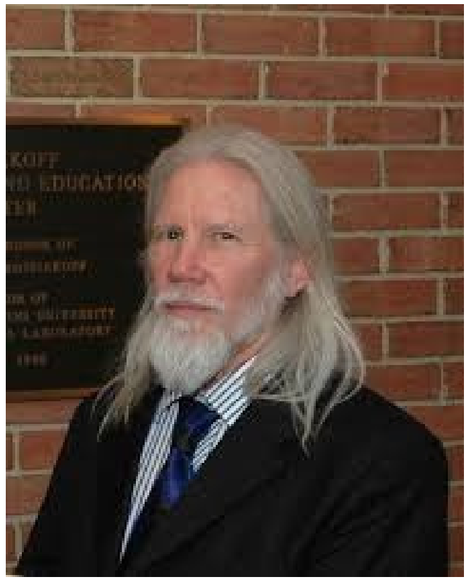
2. hafta, blokzincir teknolojisinin ortaya çıkmasında rol oynayan teknolojileri inceleyeceğiz. Eğitim sonunda uygulamalı olarak hash fonksiyonlarının nasıl çalıştığını ve Asymmetric Key teknolojisi kullanarak bir dosyanın şifrelenme ve doğrulanma süreçlerini göstereceğiz.

İçerik

- Açık Anahtar Şifrelemesi
- Dijital İmza
- Merkle Ağacı
- Kripto Cüzdanlar
- **Uygulama:**SHA256 ve .pub .key public key uygulaması

Açık Anahtar Şifrelemesi

Whitfield Diffie ve Martin Hellman, açık anahtarlı şifreleme (Public Key Cryptography / Asymmetric) kavramını tanıttı. 1976

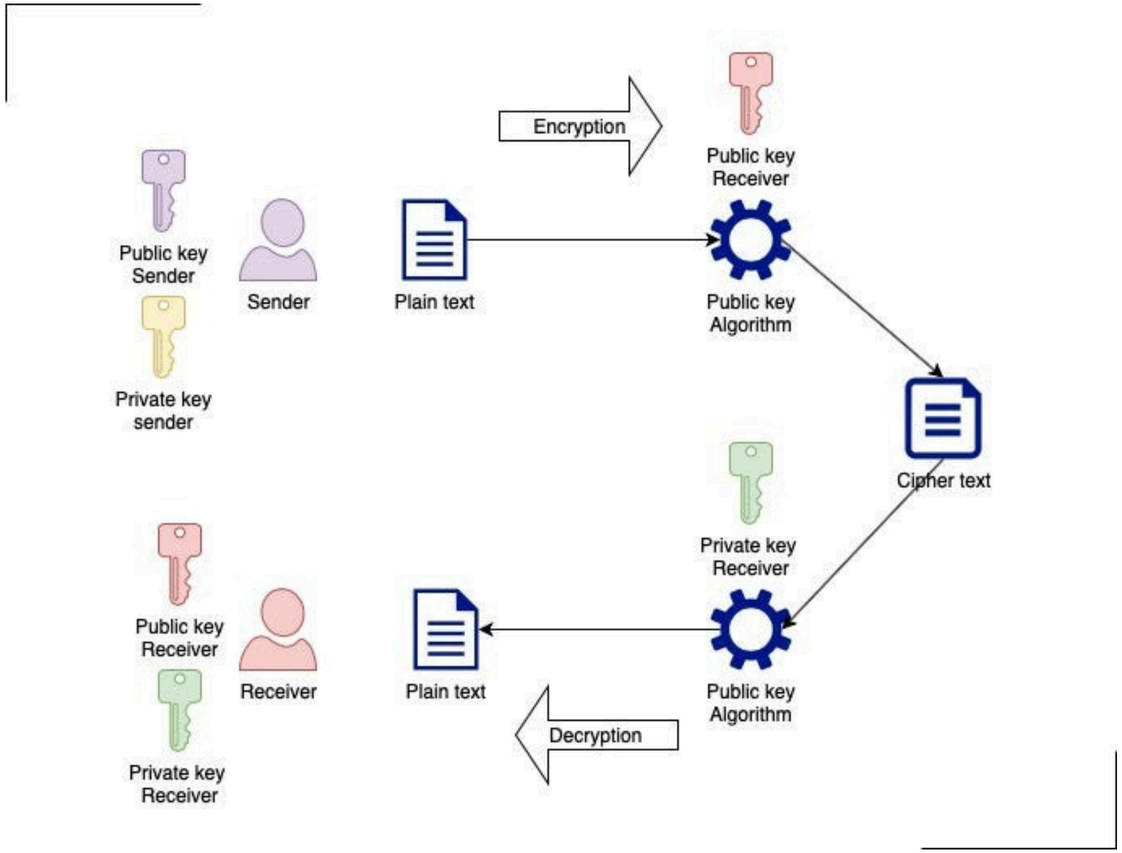


W.Diffie

M.Hellman

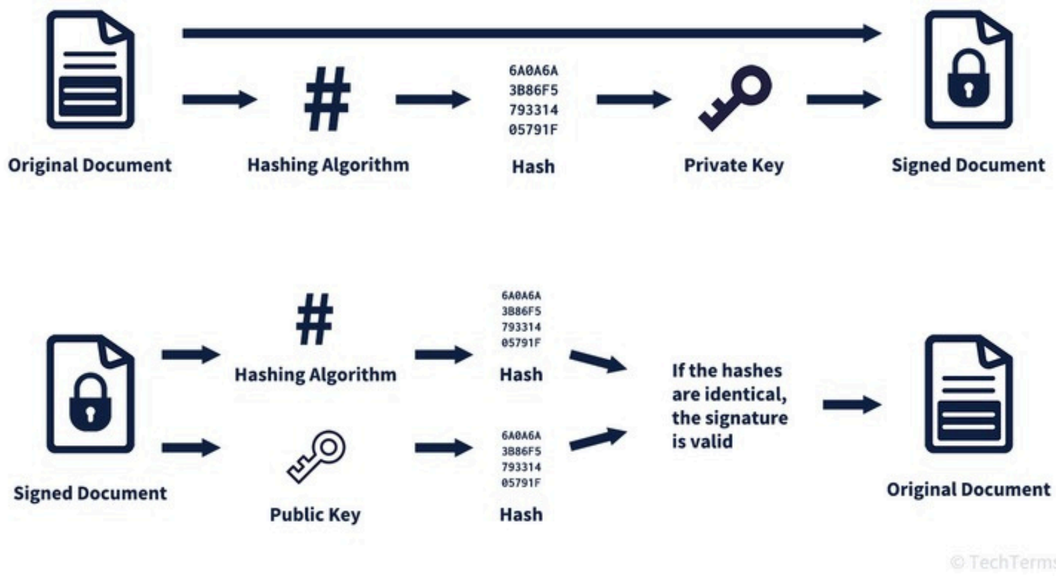
Okuma:New Directions in Cryptography

Açık Anahtar Şifrelemesi



Açık anahtar şifreleme (asimetrik şifreleme), verileri şifrelemek ve doğrulamak için bir açık anahtar ve bir özel anahtar kullanan bir kriptografi yöntemidir. Açık anahtar herkesle paylaşılabilirken, özel anahtar yalnızca sahibi tarafından saklanır ve veri güvenliği bu iki anahtarın matematiksel ilişkisine dayanır.

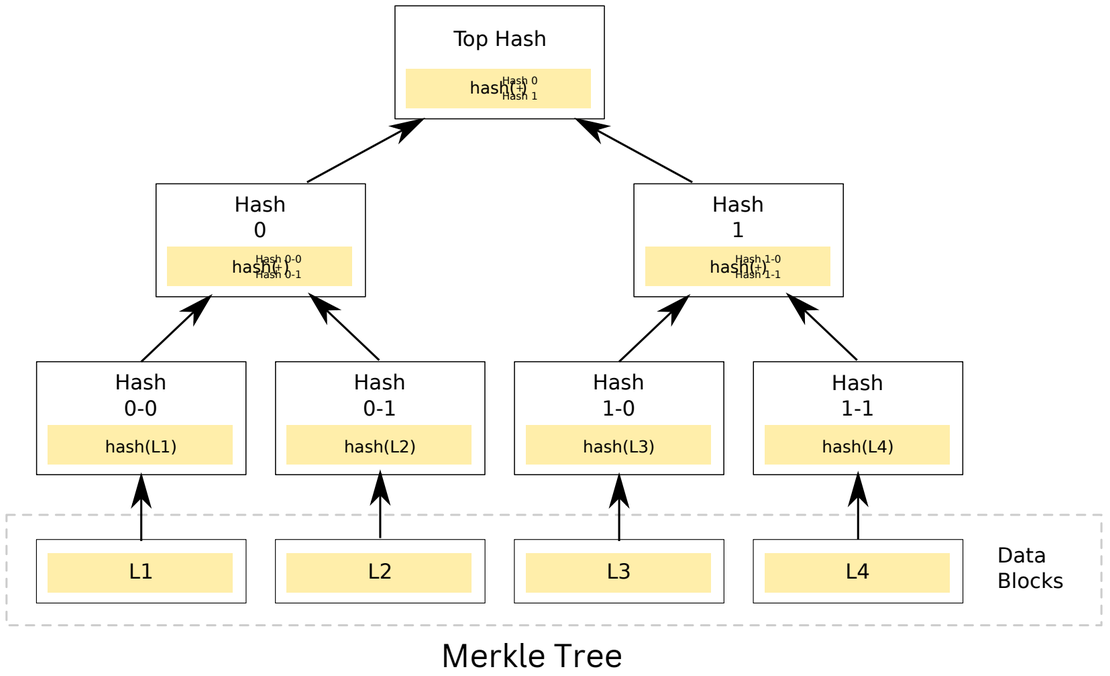
Dijital İmzalar



Dijital bir dökümanın doğruluğunu, göndericinin gerçekten o olup olmadığını onaylayan mekanizmadır. Özel anahtar ile imzalanır, açık anahtar ile doğrulanır.

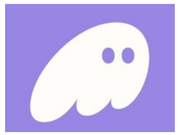
Merkle Ağacı

- İşlemleri organize etmek için Merkle ağacı (hash tree) kullanılır.
- Her işlem, SHA-256 fonksiyonundan geçirilerek bir hash değeri elde edilir.
- Hash değerleri çiftler halinde birleştirilerek yeni hash'ler oluşturulur ve bu işlem en tepeye kadar devam eder.
- Son hash, Merkle Kökü (Merkle Root) olarak adlandırılır ve blok başlığında saklanır.



Merkle Tree

Kripto Cüzdanlar



Kripto cüzdanları, private ve public keylerden oluşan ve kullanıcın ağ içerisindeki varlıklarını takip edip yönetebildiği uygulamalardır. Private keyler çok iyi saklanmalıdır çünkü bir cüzdanın private keyini bilen herkes o cüzdana sahip olur. Metamask, Phantom, Coinbase cüzdanları vb.

Uygulama: SHA256 ve Public Key

```python
import hashlib

def sha256_hash(text: str) -> str:
    """Verilen metni SHA-256 ile hashleyerek döndürür."""
    return hashlib.sha256(text.encode()).hexdigest()

# Örnek kullanım
hashed_value = sha256_hash("Merhaba Dünya")
print(hashed_value)
```

Online IDE ile test edelim

Uygulama: Dosya Şifreleme