

TEMEL KRİPTOLOJİ

İŞLEMLERİ VE

RSA, ECC

Başlıklar

- 1 Kriptografi nedir?
- 2 Temel Kriptografi İşlemleri
- 3 Simetrik - Asimetrik Şifreleme
- 4 RSA ve ECC
- 5 Java implementasyon

Kriptografi nedir?

Okunabilir durumdaki bir verinin içerdiği bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümüdür.

Amacı nedir?

Verilerimizin:

- Gizliliğini
- Bütünlüğünü
- Doğruluğunu korumaktır.



Temel Kriptografi İşlemleri

- 1 Şifreleme (Encryption)
- 2 Şifre Çözme (Decryption)
- 3 Hashing
- 4 İmzalama (Signing)
- 5 İmza Doğrulama (Verify Signing)

1) Şifreleme (Encryption)

- Veriyi anlaşılabilir hâlden anlaşılamaz hâle getirme.



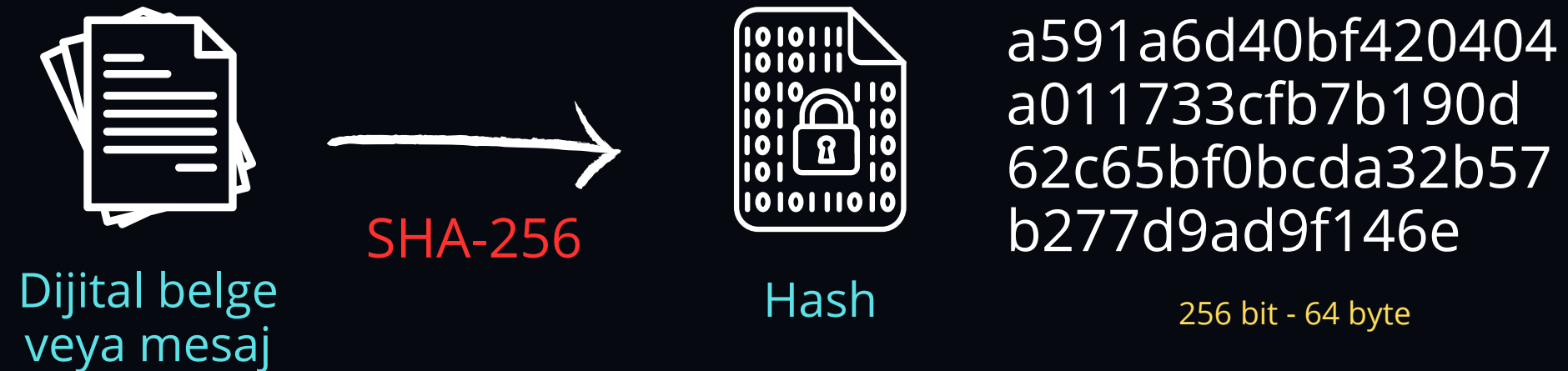
2) Şifre Çözme (Decryption)

- Veriyi anlaşılamaz hâlden anlaşılabilir hâle getirme.



3) Hashing

- Herhangi büyüklükte veriyi sabit uzunlukta ve benzersiz bir şifreye dönüştüren algoritma.

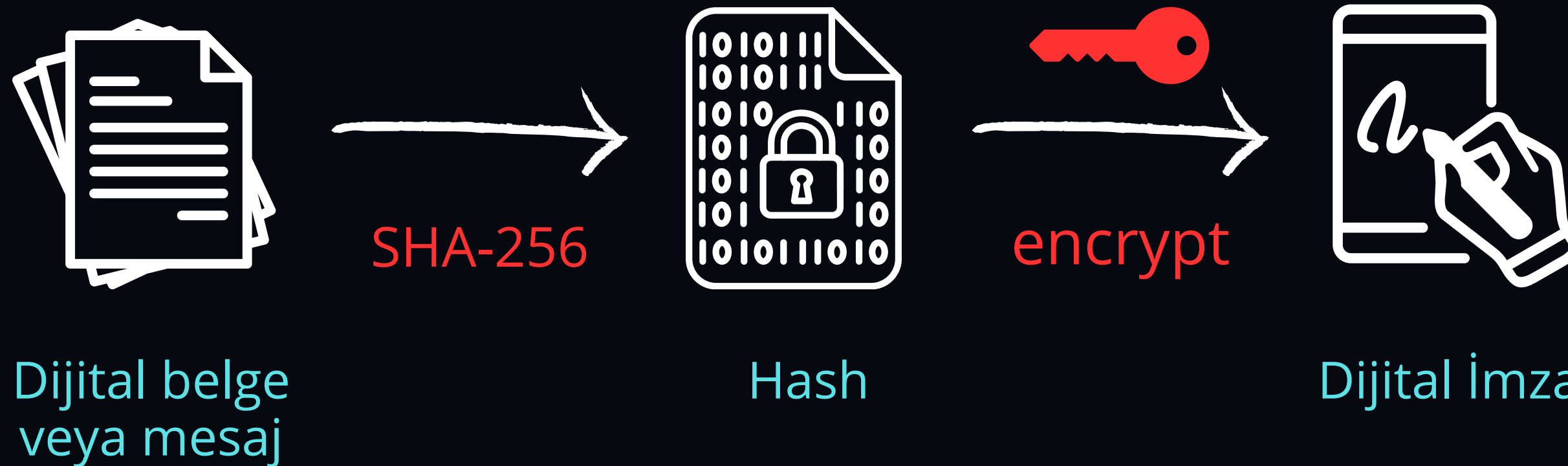


SHA-256 : Secure Hash Algorithm (256 bit)

- 256 bit çıktı
- Tek Yönlü
- Kırılması neredeyse imkansız
- Bütünlük
- Güvenlik

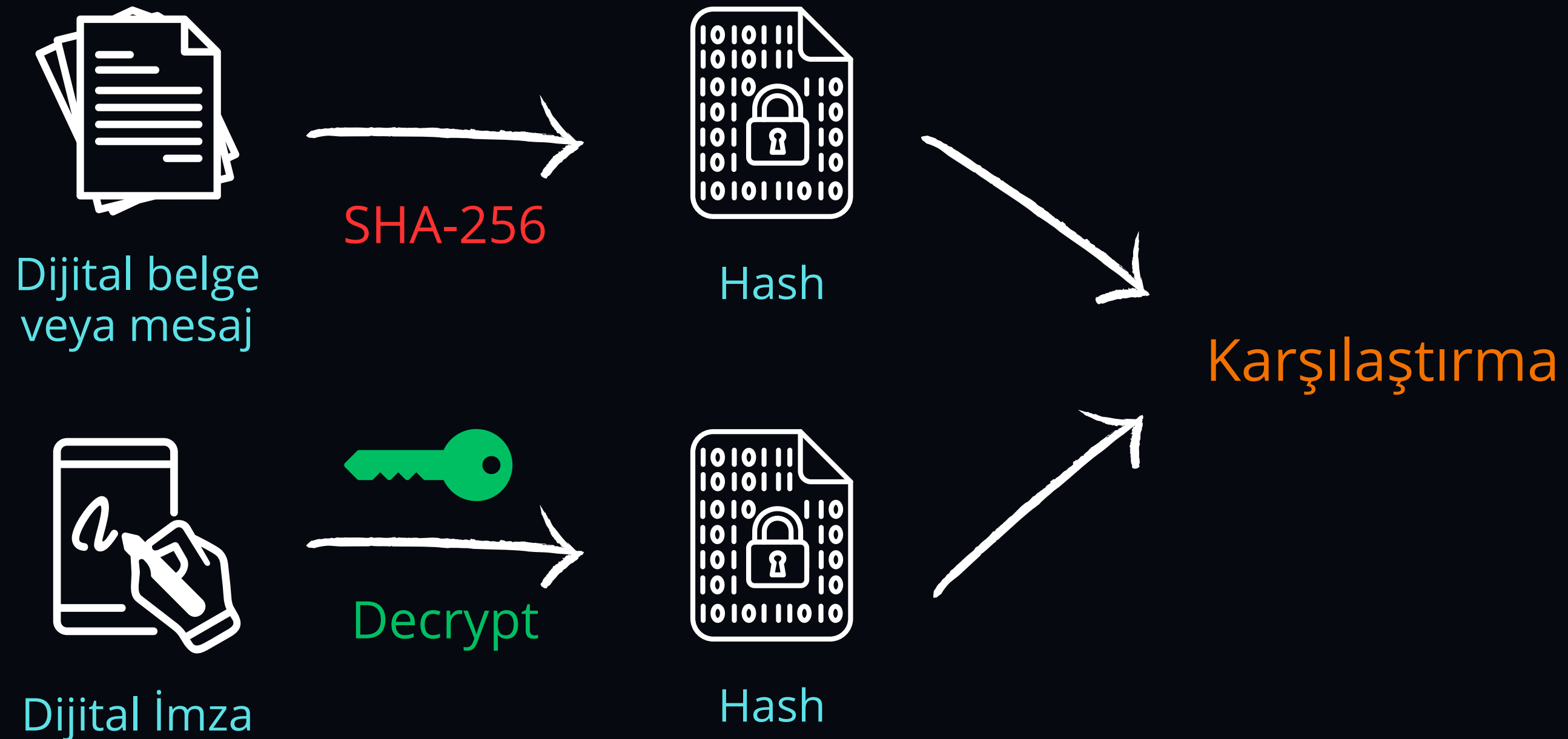
4) İmzalama (Signing)

- Dijital belge veya mesajların sahibini ve bütünlüğünü doğrulamak.



5) İmza Doğrulama (Verify Signing)




- Dijital belge veya mesajların sahibini ve bütünlüğünü doğrulamak.



Şifreleme (Encryption)







Simetrik (Symmetric)

- Tek anahtar 
- Pratik ve performanslı
- Asimetriğe göre zayıf güvenlik
- Dosya Şifreleme 
- Güvenli Mesajlaşma 
- Daha Eski
- En Yaygın Algoritma: **AES**



Asimetrik (Asymmetric)

- Anahtar çifti  
- Daha yavaş ve kaynak kullanımı fazla
- Simetriğe göre güçlü güvenlik
- Sertifika Doğrulama 
- Dijital İmza 
- Daha Yeni
- En Yaygın Algoritmalar: **RSA, ECC**

Asimetrik Şifreleme Analoji



RSA (Rivest-Shamir-Adleman)

- 1977
- İnternet güvenliği için devrim
- Çok yaygın
- Çok güvenli
- Asimetrik şifreleme algoritması



Mantığı:

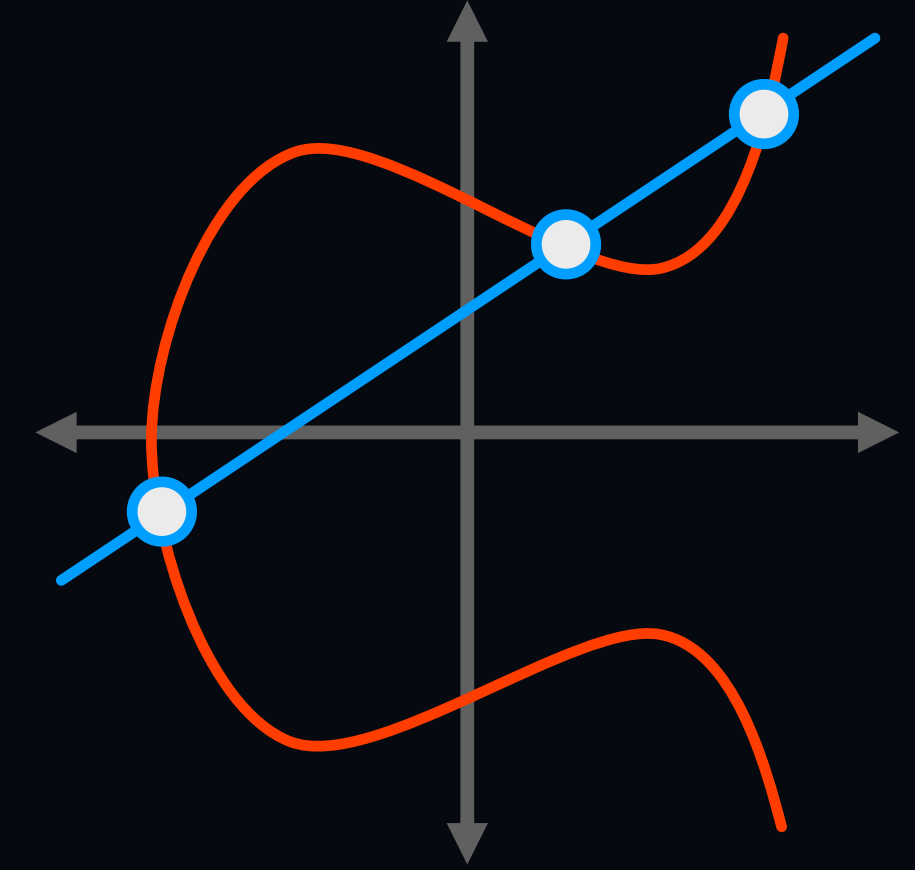
- İki oldukça büyük asal sayı seçilir ve çarpılır.
- Bu çarpım **public** ve **private** anahtarları oluşturmak için kullanılır.
- Şifreyi çözmek için çarpımı oluşturan asal sayıların bulunması gerekir.

Kullanım Alanları:

- Dijital İmzalar
- SSL/TSL Sertifikaları
- Veri Şifreleme
- Kimlik Doğrulama

ECC (Elliptic Curve Cryptography)

- 1985
- Daha modern
- Yüksek enerji verimliliği
- Mobil cihazlar için ideal
- Asimetrik şifreleme algoritması
- 3072 bit RSA ~ 256 bit ECC



Mantığı:

- Eliptik eğri denklemi üzerinde tanımlanan noktalar ve bu noktalar arasında yapılan matematiksel işlemler.
- **Private (özel)** anahtar, eliptik eğri üzerinde bir nokta ile çarpılarak **public (açık)** anahtarı oluşturur.
- Zorluğu bu seçilen noktanın belirlenememesi.

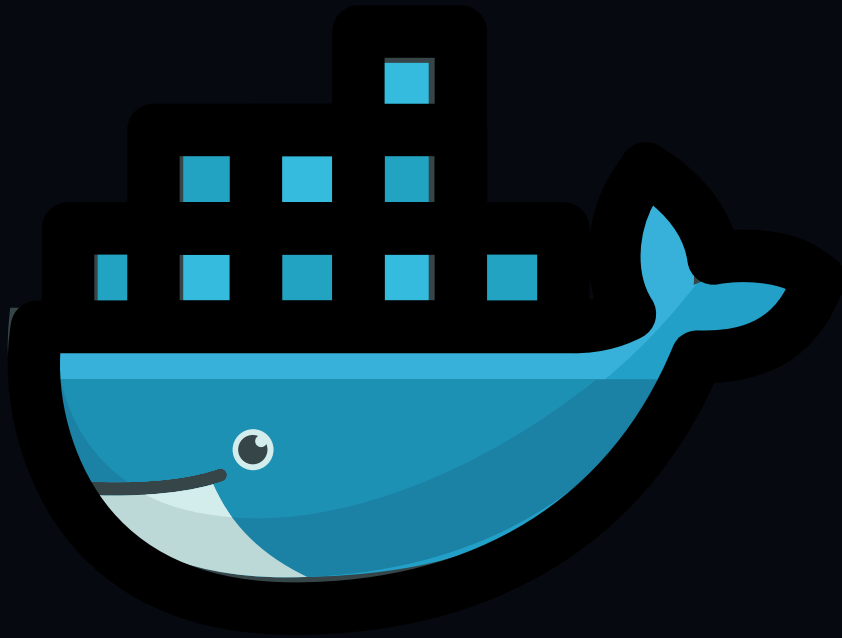
Kullanım Alanları:

- Dijital İmzalar
- SSL/TSL Sertifikaları
- Mobil ve IoT Cihazları
- Blockchain
- Kimlik Doğrulama

RSA vs ECC

Özellik	RSA (Rivest-Shamir-Adleman)	ECC (Elliptic Curve Cryptography)
Algoritmanın Temeli	Büyük sayıları asal çarpanlarına ayırma zorluğu	Eliptik eğri üzerinde nokta çarpımı
İlk Geliştirilme Tarihi	1977	1985
Anahtar Boyutu	2048-bit veya daha büyük	256-bit ile yüksek güvenlik sağlar
Performans	Daha fazla işlem gücü ve enerji tüketimi gerektirir	Düşük işlem gücü ve enerji tüketimi
Güvenlik	Daha büyük anahtar boyutlarına ihtiyaç duyar	Aynı güvenliği daha küçük anahtar boyutlarıyla sağlar
Kullanım Alanları	Dijital imzalar, SSL/TLS sertifikaları, veri şifreleme	Dijital imzalar, SSL/TLS sertifikaları, mobil ve IoT cihazları, blockchain
Verimlilik	Büyük anahtar boyutları nedeniyle daha az verimli	Daha küçük anahtarlarla yüksek verimlilik
Enerji Tüketimi	Yüksek	Düşük, mobil cihazlar ve IoT için ideal
Kuantum Bilgisayar Direnci	Kuantum bilgisayarlar karşısında daha zayıf	Kuantum bilgisayarlara karşı daha dirençli olabilir
Anahtar Üretimi ve Yönetimi	Daha büyük ve daha karmaşık anahtar yönetimi	Daha küçük, daha kolay yönetilebilir anahtarlar

Java implementasyonu



[yasirgunes/crypto_app](https://github.com/yasirgunes/crypto_app)



[yasirgunes/cryptography_operations](https://github.com/yasirgunes/cryptography_operations)

TEŞEKKÜRLER
