İmzalama Algoritmaları  
 (DSA, ECDSA, RSA)

**Özet:**

Bildiğiniz üzere günlük hayatta pek çok belgeye imzamızı atarız.Bazen bankada hesap açtırmak için , bazen bir bedel karşılığında hizmet almak bu işlemi tekrarlarız. Belgede imzamızın bulunması, ilgili işlemin **bizim tarafımızdan** yapıldığını kanıtlar. Elektronik ortamda ise bunun yerine dijital imza kullanılır[4]. Dijital imza, kimlik doğrulama amacı güden imzanın elektronik ortamdaki hali olup, elektronik ortamlarda imza yerine kullanılabilen yasal kimlik doğrulama sistemidir[5].

**Giriş:**

Dijital imzanın, ıslak imzadan farkı **belgenin içeriğine göre değişmesidir**. Bir başka deyişle, e-imza sabit bir imza değildir. İmzalanan mesaja göre benzersiz bir şekilde değişir. Ülkemizde dijital imza 5070 sayılı kanun ile **“Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri”**şeklinde tanımlanmıştır.

**DSA**

DSA algoritması da, RSA gibi açık anahtarlı bir kriptografik algoritmadır. RSA’dan farkı sadece imzalama amaçlı kullanılabilmesi, şifreleme yapılamamasıdır. DSA,  sayısal imza standardı olarak yayınlanmıştır.

**RSA**

Hem şifreleme hem de sayısal imza atma olanağı tanıyan açık anahtarlı bir kriptografik yapıdır[3]. RSA, bir asimetrik şifreleme algoritmasıdır. Asimetrik şifreleme yönteminde genel anahtar ve özel anahtar olmak üzere iki anahtar bulunur. Genel anahtar herkese açıktır. Özel anahtar ise kişiye özeldir ve sadece sahibi tarafından bilinir[1].

**Dezavantajları**

RSA algoritmasının en büyük dezavantajı, asimetrik bir şifreleme algoritması olması ve büyük sayılarla işlem yapması nedeniyle yavaş olmasıdır. Özellikle kablosuz ağ sistemlerinde bu algoritmanın kullanılması bazı sorunlara yol açabilir. Çünkü bant genişliğini fazlaca tüketir ve sistemi yavaşlatarak performans düşüşüne neden olur[2].RSA, güvenilirliği çok büyük tam sayılarla işlem yapmanın zorluğuna dayanan bir şifreleme tekniğidir. Güvenilirlik derecesi, şifrelemede kullanılan asal sayıların büyüklüğü ile orantılıdır[3].

**Avanyajları**

Simetrik şifreleme, şifrelenmiş veriyi alan tarafın veriyi deşifre edebilmesi için, gizli anahtar paylaşımını gerekli kılar. Ancak RSA asimetrik bir şifreleme tekniği olduğu için gizli anahtarın paylaşılmasına gerek yoktur. Kullanıcıların gizli anahtarlarının saklanması gerekmez. Bu da sistemi büyük bir depolama yükünden kurtarır.Büyük sayılarla işlem yapmak zor olduğu için güvenilirliği son derece yüksek olan bir şifreleme tekniğidir[2].

**ELIPTIK EĞRI DIJITAL İMZA ALGORITMASI(ECDSA)**

Eliptik Eğri Dijital İmza Algoritması (ECDSA), eliptik eğri kriptografisinden (ECC) elde edilen anahtarları kullanan bir Dijital İmza Algoritmasıdır (DSA)[5].ECDSA diğer algoritmalara göre daha verimlidir[5].Eliptik eğrilerin şifrelemede kullanılmasıdır[6]. Eliptik eğri yaklaşımı standart RSA sisteminden daha zengin matematiksel prosedürler içermektedir[6].

**ECDSA’nın Yararları**

* işlemci gücü
* saklama kapasitesi
* bant genişliği
* güç tüketimi
* Sonuç olarak, ECDSA’nin smart kartlar,cep telefonları, sayısal posta işaretleri gibi**.**

**KAYNAKÇA:**

**[1] https://www.savaskartal.com/2010/04/14/sifreleme-algoritmalari/**

**[2]http://sutod.selcuk.edu.tr/sutod/article/viewFile/120/601**

**[3]https://programsektoru.tr.gg/%26%23304%3Bmza-Algoritmas%26%23305%3B--k1-ECDSA-k2-.htm**

**[4] https://medium.com/@muhammedkaralar/dijital-i%CC%87mza-nedir-rsa-ve-dsa-nedir-617df03a97a6**

**[5]https://doubleoctopus.com/security-wiki/encryption-and-cryptography/elliptic-curve-digital-signature-algorithm/**

**[6] https://onekosmos.com/blog/the-elliptic-curve-digital-signature-algorithm/**