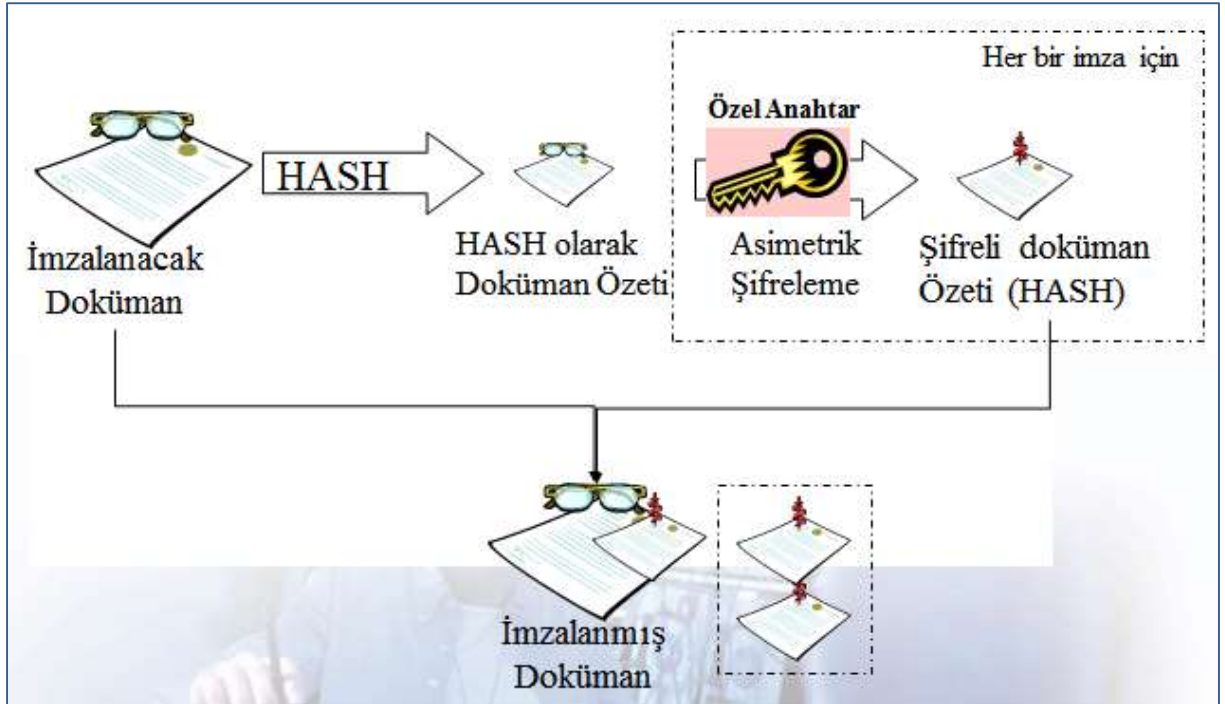


AMAÇ : Bu uygulamanın amacı kişiye açık anahtar altyapısı, e-imzalı doküman oluşturma ve e-imzalı doküman doğrulama süreçlerinin genel yapısını gösterme, basit şekilde e-imza ile doküman oluşturacak ve oluşturulan dokümanın doğruluğunu sağlayacak bir sistem oluşturmaya katkıda bulunmaktır.

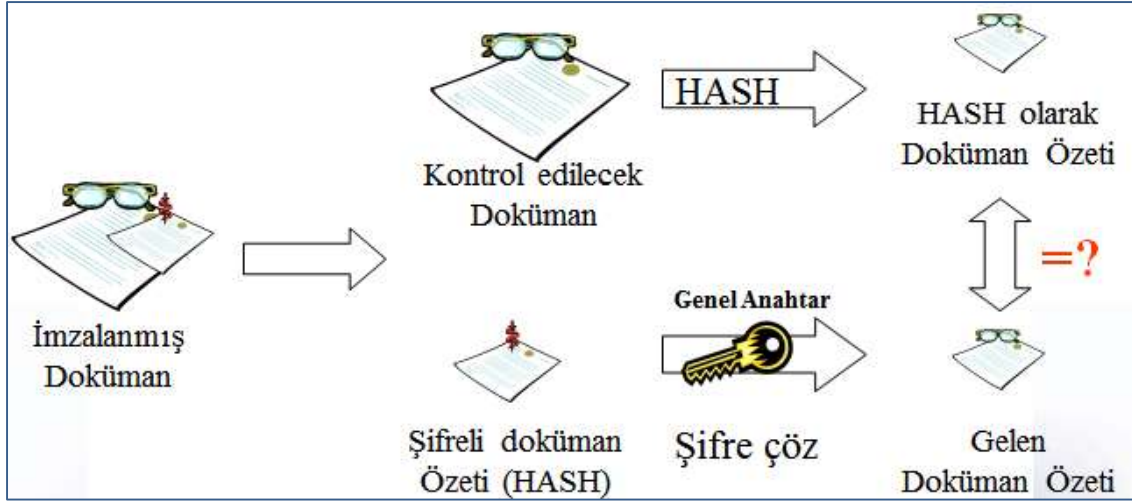
ÖNBİLGİ :

Açık Anahtar Alt Yapısı : Açık anahtar altyapısında her kullanıcı iki adet anahtara sahiptir; açık anahtar ve gizli anahtar. Bu yapı asimetrik şifreleme yöntemine göre çalışır. Metnin şifrelendiği anahtarla deşifrelediği anahtar aynı değildir. Açık anahtarlar (public key) şifrelenen veri özel (private key) anahtarla deşifrelenebilir. Açık anahtar herkes tarafından görülebilir, ulaşılabilirdir bununla birlikte özel anahtar sadece sahibi tarafından görülebilir.

E-imza Oluşturma ve Doğrulama Süreçleri : İmzalanması istenen dokümanın özet değeri çıkarılır daha sonra çıkarılan özet değeri özel anahtarla şifrelenir. Ve şifrelenmiş kısım dokümana eklenir. Oluşturulan dokümanda bulunan e-imzanın doğruluğunun tespit edilebilmesi için özel imza ile şifrelenen özet değeri açık anahtar (public key) ile deşifrelenir, elde edilen değer dokümanın özet değeri çıkarılarak karşılaştırılır. Karşılaştırma sonucu bize dokümanın belirtilen kişi tarafından imzalandığını gösterir.



Şekil 1 E-İmza Oluşturma Süreci



Şekil 2 E-İmza Doğrulama Süreci

UYGULAMA :

A. Uygulama öncesi yapılacaklar :

Asimetrik anahtar_oluştur (yaklaşık_p_değeri) → açık_anahtar, özel anahtar

Yukarıda yaklaşık p değerini kullanarak açık ve özel anahtar oluşturan asimetrik anahtar oluştur fonksiyonunu tasarlayıp kodlayınız.

B. Uygulamanın Yapılışı:

Doküman_imzala (doküman, özel_anahtar) → E-imzalı_doküman

Doküman_doğrula(e-imzalı_doküman, açık anahtar) → Doğru / Yanlış

Yukarıda verilen parametrelere göre doküman_imzala ve doküman doğrula fonksiyonlarını tasarlayıp kodlayınız. Oluşturulan fonksiyonları doküman imzalamak için kullanıp sonuçlarını gözleyiniz. Dokümanların imzalanmasında açık ve özel anahtar olarak daha önce oluşturduğunuz asimetrik şifreleme anahtar oluşturma fonksiyonunu kullanınız.

ANALİZ :

- Oluşturulan e-imzalı doküman için güvenlik seviyesini tartışınız.
- Asimetrik anahtar oluşturulması sürecinde p değerinin küçük veya büyük olmasını, varsa eşik değerini tartışınız.