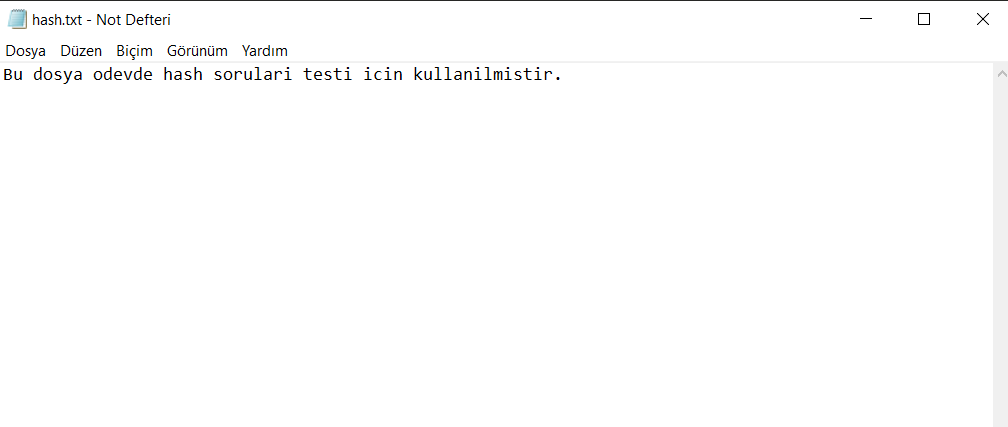
PART3-)

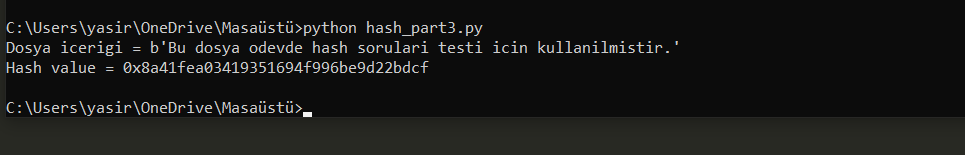
Hash fonksiyonunun çalıştığını ve nasıl gerçekleştirildiğini bir txt dosyasının değişip değişmediğini kontrol ederek kullandım.

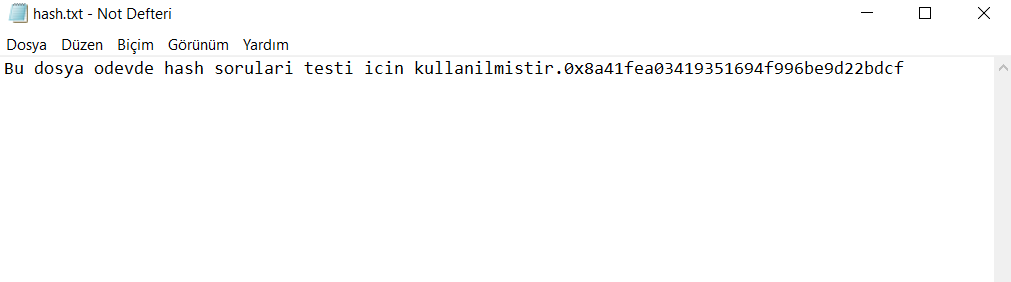
Part3 de ilk olarak dosyayı okuyorum. Daha sonra okuduğum dosyayı hex değerlerine çeviriyorum ve hashing fonksiyonuna gönderiyorum. Hashing fonksiyonunda part2 de gerçekleştirdiğim aes nin cbc si modunu kullanarak hash işlemi yapıyorum. Cbc moduyla şifrelenmiş mesajın sadece son blok çıktısını alıyorum çünkü cbc modda geri besleme olduğu için tüm bitler son bloku etkilemiş oluyor. Yani hash fonksiyonunda giriş uzunluğum ne olursa olsun çıkış uzunluğu 128 bit oluyor. Sonra bu hash değerini ekrana yazdırıp dosyaya ekliyorum.

Test verilerden çıktıyı inceliyecek olursak;

Örneğin program öncesi bu benim txt dosyam:



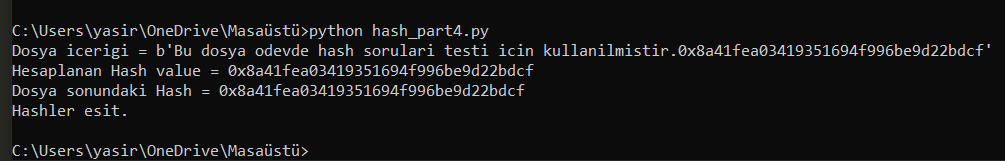
Bu txt dosyası için programımı çalıştırdığımda şöyle bir çıktı alıyorum:

Ekrana okunan dosyanın içeriğini ve o dosyayı kullanarak oluşturulan hash değerini yazıyorum. Ayrıca program bitmeden bu hash değerini dosyanın sonuna ekliyor.

PART4-) Şimdi part4 de dosyanın değiştirilip edilmediğini test ediyorum.

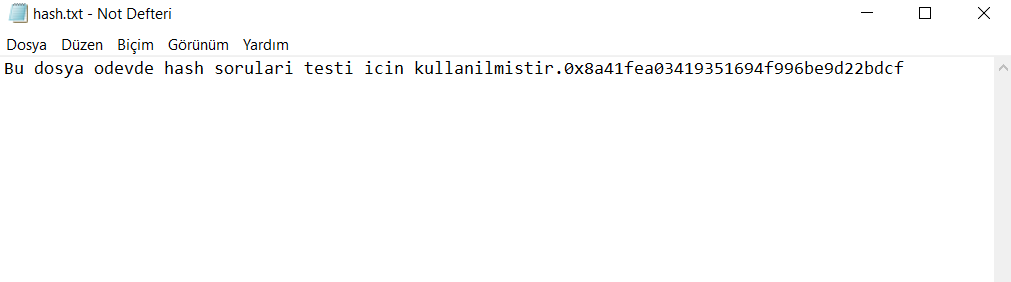
Part4’de tekrar sonuna hash kodu eklenmiş dosyayı okuyorum ve hash kodsuz kısmın hashini hesaplıyorum. Daha sonra dosyanın sonuna eklenmiş Hash kodu ile yeni bulduğum hashi karşılaştırıyorum.Eğer hashler eşit ise dosya değiştirilmemiş demektir, Hashler farklı ise dosya değiştirilmiş demektir.

Part3 programını çalıştırdıktan sonra dosyayı hiç ellemiyorum ve part4 kodunu çalıştırıyorum ve böyle bir çıktı alıyorum:

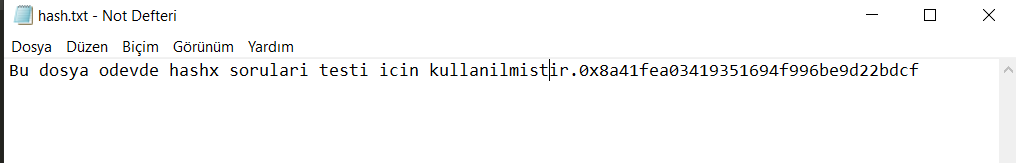


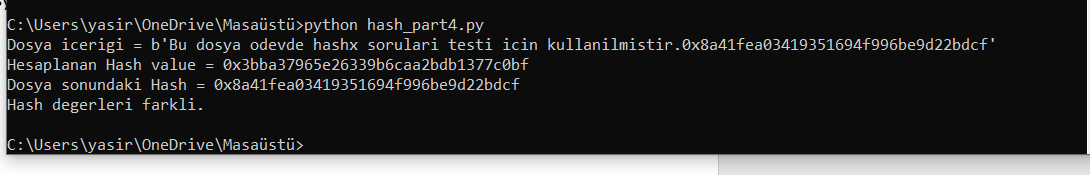
Görüldüğü üzere kodun tekrar hashini hesaplıyorum ve part3 ün çalıştırılması ile dosya sonuna eklenen hash ile karşılaştırıyorum ve değerler aynı çıkıyor. Demekki dosyam değiştirilmemiş.

Ama part4 ü çalıştırmadan önce dosyayı değiştirirsem:

Değiştirilmemiş dosyam by iken:

Dosyayı değiştirip bu hale getiriyorum. Görüldüğü üzere değişiklik olarak sadece ‘hash’ kelimesini ‘hashx’ yaptım.



Bu değişiklik ile dosyamı değiştirdikten sonra tekrar part4 kodunu çalıştırıyorum:

Görüldüğü gibi sadece ‘hash’ kelimesini ‘hashx’ yaptığım da hash değeri çok değişti ve farklı bir değer çıktı. Program bu sayede dosyanın değiştiğini anlıyor ve hash değerleri farklı yazıp programı sonlandırıyor.

Kodlarım python 3.8.5 versiyonunda yazılmıştır.