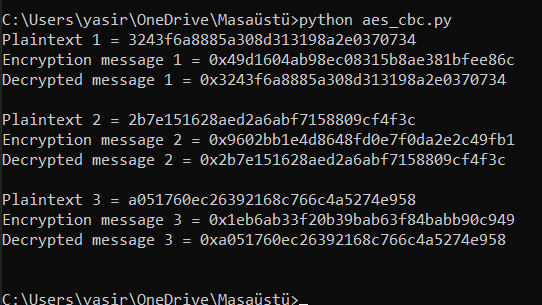
Part2) Bu kısımda part1 deki AES yapımı kullandım. Sadece AES’yi cbc ve ofb modda çalışabilcek hale getirdim. İlk olarak cbc modunu inceleyelim:



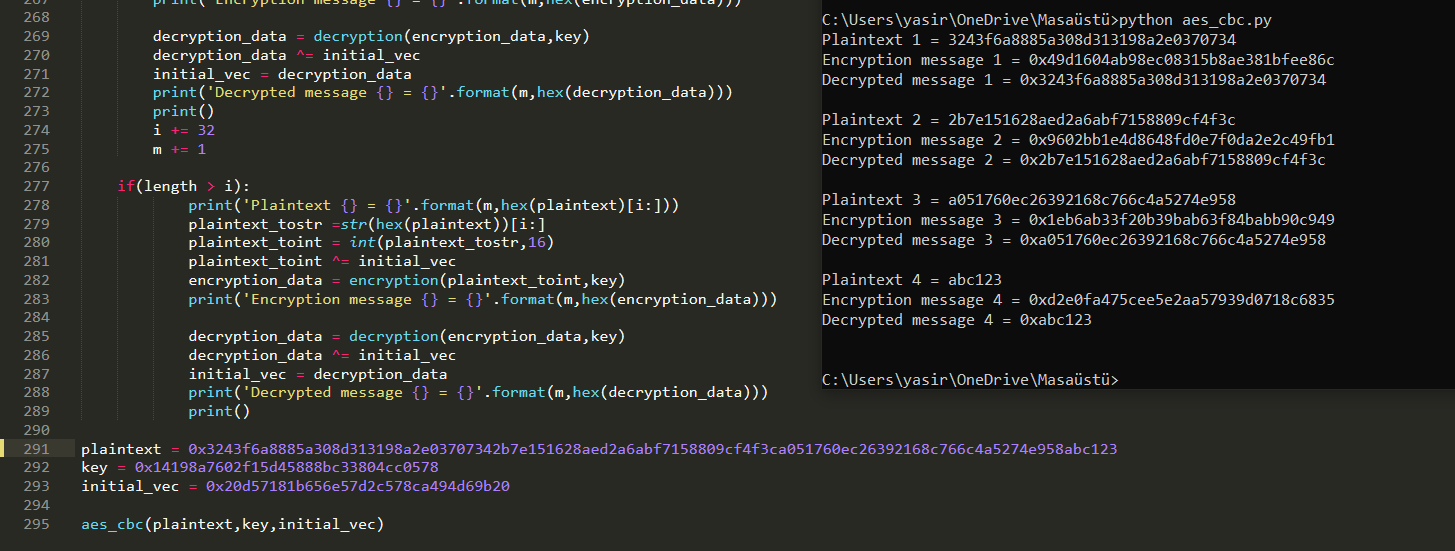
Cbc modunda yapıda olduğu gibi bir initial\_vector kullandım, bu initial vector ile plaintexti mi 265. Satırla xor işleminden geçirdim ve sonucu aes ile şifreledim. Deşifreleme kısmında işe şifrelenmiş veriyi decryption algoritmasına gönderdim ve gelen veriyi initial vector ile xor işlemine tabi tuttum. Bu sonuç benim deşifrelenmiş mesajım olmuş oldu son olarak ise initial vektörümün yeni değeri olarak cbc mod yapısında olduğu gibi deşifrelenmiş mesaj olarak atadım. Bu şekilde uzun bir plaintexti tekrarlamalı aşamalar ile cbc modunu kullanıp şifreleyip deşifreledim. Son olarak döngüden sonra bir if ile artık bit var mı onun kontrolünü yapıp ona göre işlem yaptım. Bu sayede plaintextim illa 128 bitlik değerler içermesine gerek yok. Mesela cbc modda son bloka 128 bit değilde 60 bit gitse bile çalışır. Bu sayede plaintextin uzunluğundan bağımsız çalışabilir.

Kodun çıktısına bakıcak olursak :



Bu şekilde bir çıktı alıyorum. Görüldüğü üzere tekrarlamalı bir şekilde blok blok textler şifrelenmiş halleri ve deşifrelenmiş hallerini ekrana yazdırdım. Decrypted messajlar görüldüğü üzere plaintextin blok blok bölünmüş halleri oldu.

Daha sonra plaintextimin sonuna hex abc123 değerini ekledim sadece 128 bitin katlarında çalışmadığını göstermek için



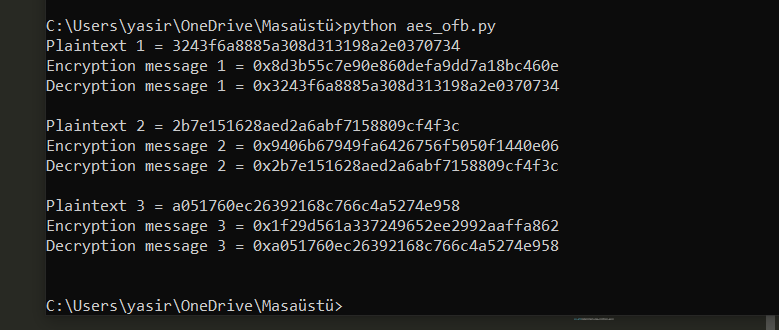
Ve görüldüğü üzere yapıp boyuttan bağımsız çalışabildi. Son bloka sadece abc123 değeri gitmesine rağmen başarı ile şifreleyip deşifre edilebildi.

Şimdi OFB kodumu inceleyelim:



OFB’de CBC modumdaki algoritmama benzer, burada da bir initial vector kullandım ve ilk olarak satır 246 da plaintextimi değilde initial vectorumu encryption algoritmasına tabi tuttum. Daha sonra ciphertextimi bu değer ile plaintextimin xorlanmasından elde ettim. Deşifrelenmiş mesaj ise ciphertext ile initial vektörün xorlanması ile elde edildi. Ayrıca görüldüğü üzere OFB yapısında olduğu gibi hem şifreleme için hem deşifreleme için encryption algoritmasını kullandım.

Kodu çalıştırdığımda aldığım çıktıyı incelicek olursak:



Görüldüğü üzere Bloklar halinde CBC modda olduğu gibi plaintextimi şifrelenmiş halii ve deşifrelenmiş halini ekrana yazdırdım. Deşifrelenmiş mesajlarım plaintextimi oluşturuyor. Ayrıca bu modda CBC gibi plaintext uzunluğundan bağımsız çalışabiliyor. Son bloka 128 bitden daha kısa bit veri gelse bile çalışıyor.

Kodlar python 3.8.5 versiyonun da yazılmıştır.