

**COMPUTER SYSTEM SECURİTY DERSİ**

**1.ÖDEV RAPORU**

AHMET İHSAN SAVAŞ

14121221028

**1.PROJENİN AMACI**

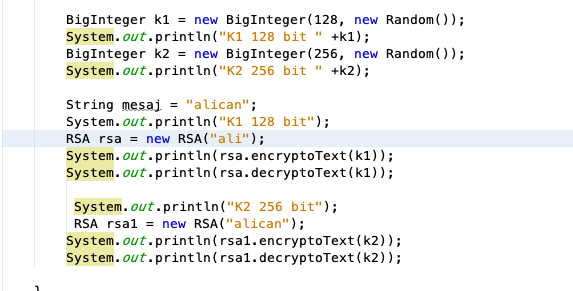
Bu projemizde bizden istenen derste öğrenmeye çalışmış olduğumuz RSA , AES , DES vb. şifreleme tekniklerini ve SHA256 metoduyla dijital imza tekniğini uygulamaya dökmemiz istenmektedir. Bu doğrultuda bizden istenenleri yapmaya çalıştım.

**2.PROJE SORULARI**

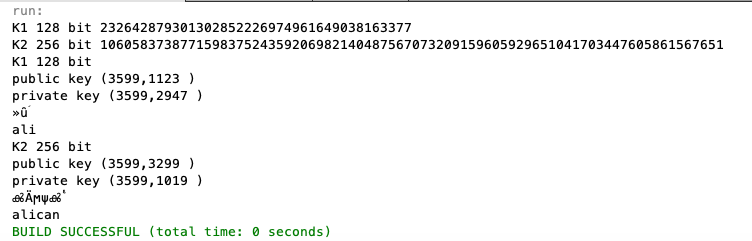
1. Birinci soruda bizden public ve private key oluşturmamız istenmektedir. Bende bu doğrultuda ilk öncelikle RSA da p ve q keylerini seçip daha sonra n,z,e yi bulmaya çalıştım ve daha sonra Public ve Private Keylerini yazdırdım. Key generator yerine dersteki gibi p,q asal sayılarından belirli işlemler yapıp public ve private keyleri elde ettim.



**2-** İkinci Soruda bizden 128 Bit K1 ve 256 bit K2 oluşturup bizden public ve private key lerle kullanmamızı ve RSA Uygulamasını yapmamız istenmektedir. Bu doğrultuda public ve private keyden farklı olarak Big Integer kullanarak random K1 ve K2 oluşturdum. Daha sonra encryptText() metoduna key parametrelerini vererek çıktı elde etmeye çalıştım.



K1 ve K2 keyleri kullanılarak şifrelenen metinlerden Aşağıdaki çıktıyı elde ettim.

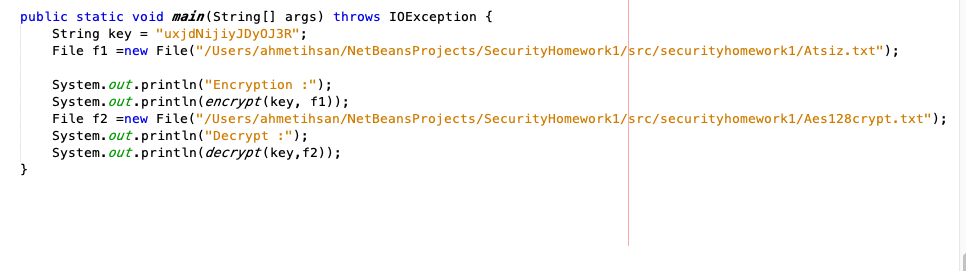


**4-** Bu soruda bizden AES 128 bit CBC , AES 256 bit CBC ve DES 56 bit CBC teknikleri kullanılarak 1.MB büyüklüğündeki dosyayı her bir şifreleme algoritmasını kullanarak şifrelememiz gerekmektedir ve aralarında karşılaştırma yapmamız istenmektedir. Bende “Atsiz.txt “dosyasını bu nedenle kullandım .

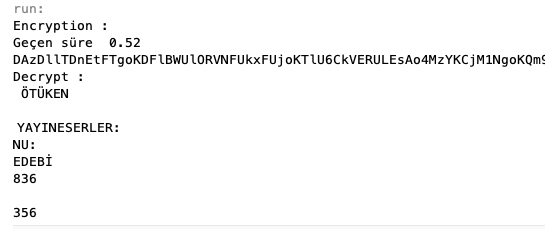
Öncelikle AES 128 Bit ve AES 256 bit arasında ki fark key uzunluğundan kaynaklamaktadır. AES 128 bit veriyi 128 bit blok uzunluğu ile şifrelerken AES 256 veriyi 256 bit veriyi 256 blok uzunluğunda şifreler.

İlk olarak “Atsiz.txt “dosyasını şifreleyerek “Aes128.txt” dosyası haline getirdim ve decrypt metoduna parametre olarak gönderdim, daha sonra da “Aes128decrypt.txt” dosyası ekranda yazdırdım. Aynı işlemleri AES256 ve DES56 için de yaptım.

i)AES 128 cbc



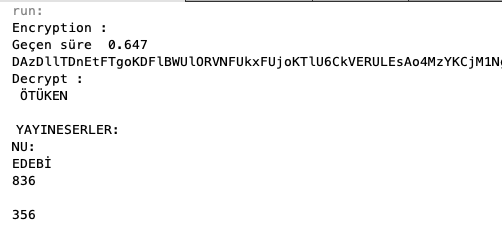
Aes 128 bit cbc için encrypt işlemi 0.52 saniye sürmüştür.



ii) AES 256 Bit CBC



AES 256 CBC Çıktısı;



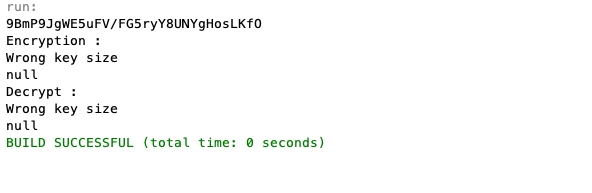
Şifreleme işlemi AES 128 bit te 0.52 sn. , AES 256 bit te ise 0.647 sn. sürmüştür. Böyle olmasının ana nedeni key size dan dolayıdır ,key size ın büyük olmasından dolayı her 256 bit için şifrelediğinden daha fazla tur sayısı yapması gerekmektedir ve bu yüzden AES 256 Bit işlem değeri daha yüksektir.

iii) DES 56 CBC

AES te yaptığım işlemlerin aynısını DES için de yaptım fakat DES hiçbir türlü key kabul etmedi. Bende farklı paading kullandım anca yine aynı hata ile karşılaştım.



DES key size dan dolayı aldığım hata.



AHMET İHSAN SAVAŞ

1421221028