Açık SSL Dosyaları Şifreleme ve Şifre Çözme

Gerekli tahmini süre: 15 dakika

Bu laboratuvar çalışmasında, özel hash teknikleri kullanarak dosyaları okunamaz, anlaşılmaz bir formata şifrelemeyi ve ayrıca şifrelenmiş bir dosyayı şifre çözmeyi öğreneceksiniz.

Öğrenme Hedefleri

Bu laboratuvar çalışmasını tamamladıktan sonra şunları yapabileceksiniz:

- Şifrelenmiş bir dosyayı indirmek ve ardından şifresini çözmek
- Dosyalarınızı şifrelemek için özel ve gizli anahtarlar oluşturmak
- Şifrelenmiş dosyaların şifresini çözmek
- Şifreleme standardını güçlendiren 2500 yineleme ile şifreleme uygulamak.

Ön Koşullar (isteğe bağlı)

Linux komut istemcisini kullanma konusunda aşina olmak.

Görev 1: Basit bir dosyanın şifresini çözme

Adım 1:

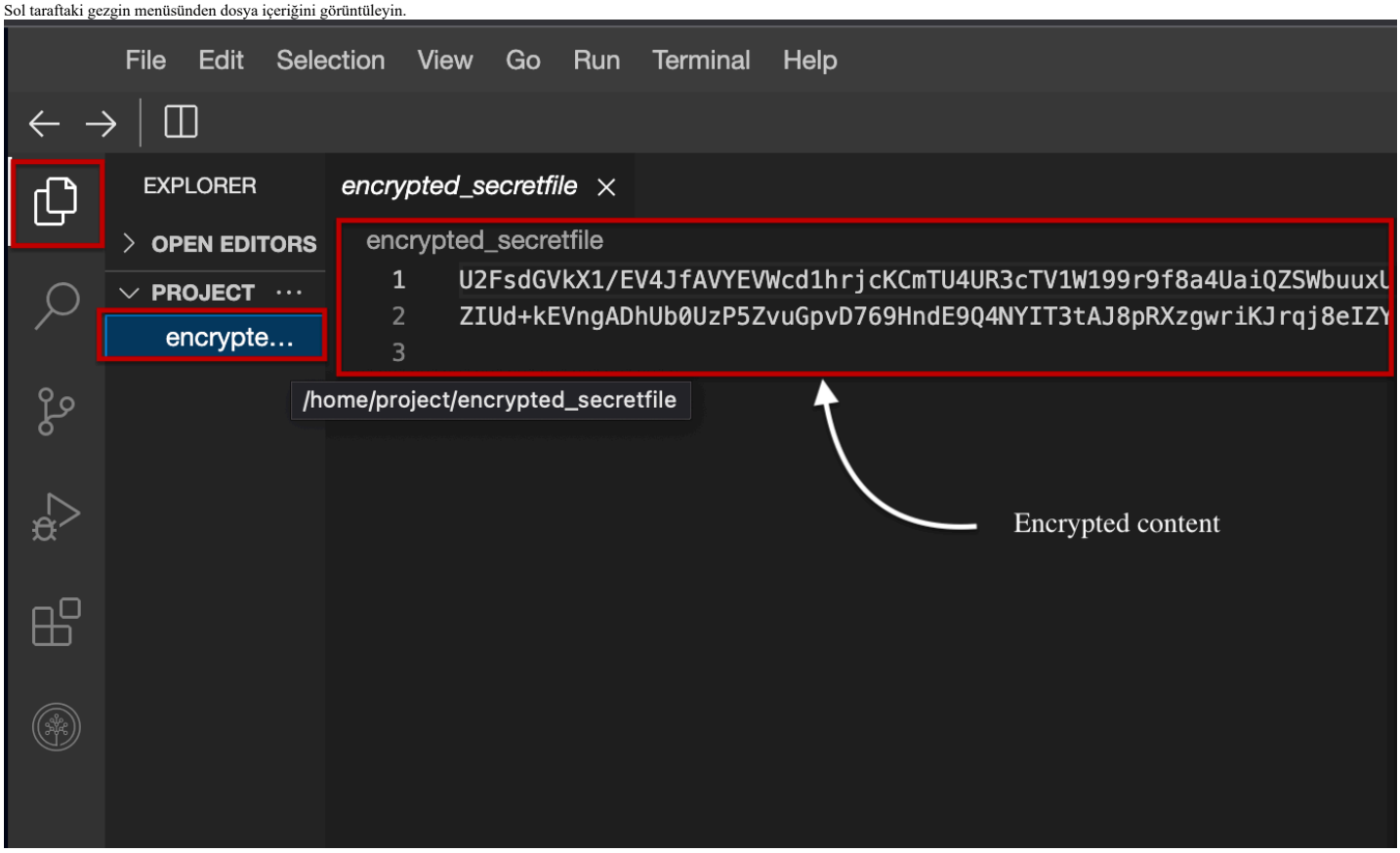
Sağdaki terminalde aşağıdaki komutu çalıştırarak şifreli bir gizli dosya elde edin.

```
wget https://cf-courses-data.s3.us.cloud-object-storage.appdomain.cloud/IBM-CD0267EN-SkillsNetwork/labs/module1/encrypted_secretfile
```

Bu, dosyayı yerel ortamınıza indirecektir.

Adım 2:

Sol taraftaki gezgin menüsünden dosya içeriğini görüntüleyin.



İçeriğin okunabilir olmadığını ve tamamen şifreli olduğunu göreceksiniz. Bu, aes-256-cbc şifreleme algoritması kullanılarak kodlanmıştır. Her şifrelemenin kendine ait bir algoritması vardır. aes-256-cbc, daha eski ve daha basit şifrelerden biridir ve verileri şifrelemek için şimdi çok daha iyi algoritmalar mevcuttur.

Adım 3:

Dosyayı deşifre etmek için aşağıdaki komutu çalıştırın.

```
openssl aes-256-cbc -d -a -pbkdf2 -in encrypted_secretfile -out secrets.txt
```

Komut seçeneği	Anlamı
aes-256-cbc	Şifreleme algoritması
-d	Şifre çözme
-a	Base64 çözümleme
-pbkdf2	Parola tabanlı anahtar türetme fonksiyonu 2 kullanın
-in encrypted_secretfile	Girdi dosyası
-out secrets.txt	Çıktı dosyası

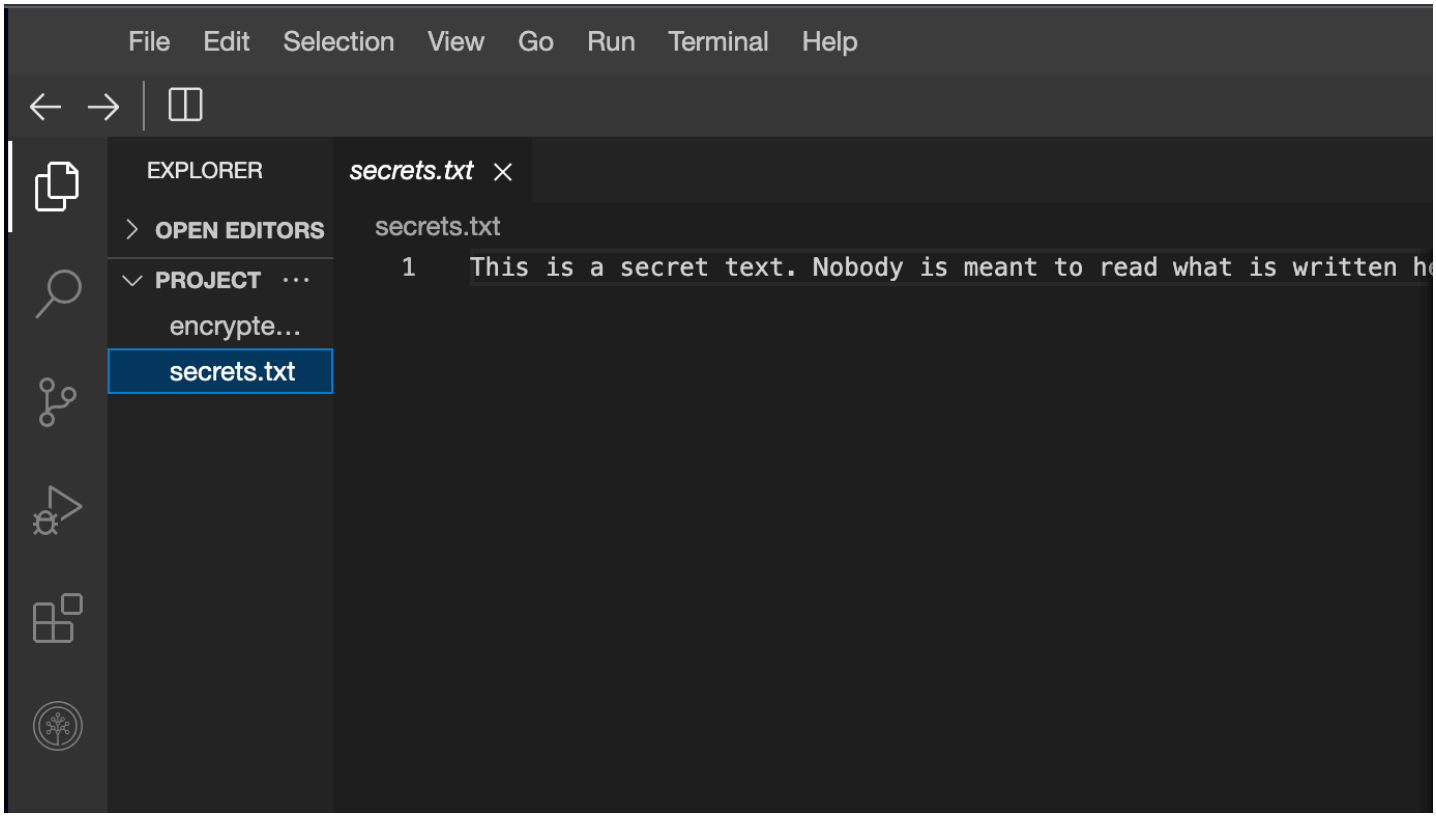
Adım 4:

Sizden bir parola girmeniz istenecektir. Dosya şifrelendiğinde, aes-256-cbc şifreleme algoritması kullanılarak bir parola ile şifrelendi. Dosyayı şifrelemek için parolayı isteme alanına yazmalısınız. Dosya `adios` parolası ile şifrelendi. Aynısını vermeniz gerekiyor.

Parolayı yazın ve enter tuşuna basın. Parolanın terminalde görünmeyeceğini unutmayın.

Adım 5:

Şifrelenmiş dosya, şifre çözülmüş içeriği ile birlikte gezginde görüntülenebilir.



Görev 2: Dosyayı Şifrele

Artık dosyayı şifre çözdüğünüze göre, dosyayı şifrelemeye devam edin.

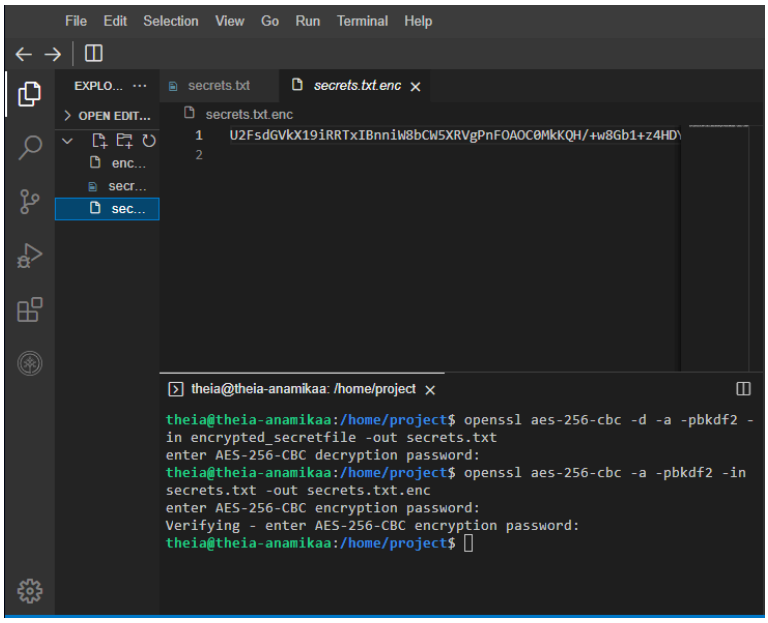
Adım 1:

secret.txt dosyasında gerekli değişiklikleri yapın ve yeni bir şifre ile şifreleyin. Şifreyi doğrulamak için aynı şifreyi girmeniz istenecektir. Şifreyi hatırladığınızdan emin olun.

```
openssl aes-256-cbc -a -pbkdf2 -in secrets.txt -out secrets.txt.enc
```

Adım 2:

Artık, secrets.txt.enc dosyasını görüyorsanız, bu dosyada şifrelenmiş içerikler olacaktır.



Adım 3:

Aşağıdaki komutu çalıştırarak orijinal `secret.txt` dosyasını sistemden kaldırın.

```
rm secrets.txt
```

Zorluk:

Görev 1'de belirtilen talimatları **Adım 3**'ten başlayarak takip edin ve ardından dosyayı şifre çözmek ve içeriğini görüntülemek için sonraki adımlara devam edin.

Not: Burada, *Adım 4*'te verilen şifreden farklı yeni bir şifre belirlemeniz gerekmektedir.

Görev 3: Şifreleme Seçeneklerini Değiştirme

1. Dosyayı kolayca çözülemeyecek bir şekilde şifrelemek için yine de yineleme sayısını daha yüksek sayılara ayarlayabiliriz. Birçok yineleme, şifrelenmiş dosyayı brute-force ile çözmek için gereken süreyi artırır.

```
openssl aes-256-cbc -a -pbkdf2 -iter 2500 -in secrets.txt -out secrets_2500.txt.enc
```

Şifrelenmiş dosyanın içeriğinde farklı bir yineleme sayısı kullandığınızda bir değişiklik gözlemleyeceksiniz.

Sonuç

Tebrikler! Artık dosyaları şifrelemeyi ve şifre çözmeyi öğrendiniz.

Sonraki Adımlar

Terminalde aşağıdaki komutu yazarak OpenSSL ile mevcut şifreleme algoritmalarını keşfedebilirsiniz.

```
openssl enc --list
```

Yazar(lar)

Lavanya T S

Değişiklik Günlüğü

Tarih	Versiyon	Değiştiren	Değişiklik Açıklaması
2023-12-20	0.5	Sowmyaa Gurusamy	Talimatlar güncellendi
2023-09-18	0.4	Dania Kulsum	Çıktı ekran görüntüsü eklendi
2023-08-09	0.3	Mary Stenberg	Düzenlemelerle QA Geçişi
2023-08-07	0.2	Gagandeep Singh	ID incelemesi

Tarih	Versiyon	Değiştiren	Değişiklik Açıklaması
2023-07-31	0.1	Lavanya T S	İlk sürüm oluşturuldu