Kriptografi Dönem Ödevi

Teslim tarihi: 6 Mayıs 2020

Gönderim şekli: https://github.com/nyucel/kriptografi adresine Pull Request olarak gönderilmelidir.

Gruplar: Gruplar en fazla üçer kişiden oluşacaktır. 21 Nisan tarihine kadar bir grup oluşturup nyucel@comu.edu.tr adresine göndermezseniz ödevi tek başınıza tamamlayacağınızı kabul edeceğim. Her dosyanın içerisinde hazırlayanların adları birer yorum satırı olarak buunmalıdır. Eğer bir grup halince çalışılmışsa dosyanın ilk gönderiminden sonra grubun üyeleri kendi isimlerinin eklenmesini yine ayrı birer Pull Request ile sağlamalıdır.

Programlama dili: Yazacağınız kodları python3 ile yazmanızı bekliyorum.

Kullanılabilecek modüller: Temel python kitaplıklarının yanında yukarıda verilen adresteki functions.py dosyasındaki isprime ve allprimes fonksiyonlarını içe aktarıp kullanabilirsiniz. İhtiyacımız olduğunda gerekli yeni fonksiyonları kendiniz yazıp kullanabilirsiniz. pip benzeri paket yöneticileri ile ilave bir modül yüklemeden önce mutlaka elektronik posta ile bana durumu bildirin.

Her grup için ayrı bir açık anahtarlı kriptosistem belirlenecek ve grupların bu kriptosistemler için anahtar üretimi, şifreleme ve deşifreleme işlemlerini gerçekleştiren bir python modülü göndermeleri beklenecektir.

Hazırlayacağınız modül üç adet fonksiyon içermelidir:

- **keygen**(n)
  - Bu fonksiyon n'i bit degeri olarak almalıdır. Örneğin n = 32 olduğunda 32 bitlik bir anahtar çifti üretmelidir. Her çağırılışında publickey.txt ve privatekey.txt dosyalarını adlarına uygun bir şekilde üretmelidir.
- **encrypt**(plaintext, publickey.txt)
  - Bu fonksiyon plaintext dosyası içindeki metni publickey.txt dosyası içinde oluşturulmuş olan anahtarla şifreleyip ciphertext dosyasına yazmalıdır.
- **decrypt**(ciphertext, privatekey.txt)
  - Bu fonksiyon ciphertext dosyası içindeki metni privatekey.txt dosyası içindeki özel anahtarla deşifreleyip plaintext2 dosyasına yazmalıdır. Çalışmasını tamamladıktan sonra aynı dizinde bulunan plaintext ve plaintext2 dosyalarını karşılaştırıp özdeş olup olmadıklarını konsol çıktısı olarak vermelidir.

encrypt ve decrypt fonksiyonları çağırıldıklarında publickey.txt ve privatekey.txt dosyaları mevcut değilse önce keygen fonksiyonunun çalıştırılması gerektiği uyarısını vermelidir.

Her üç işlem de 1 dakikadan kısa sürede çalışmasını tamamlamalıdır.

Yazdığınız modüller kendi başına çalıştırılmayacak olduğundan fonksiyon adları ve aldığı parametreleri yukarıda olduğu gibi kullanmanız önemlidir.

Eğer bu süreçte internet bağlantınız olmayacaksa ve bu dosyayı çevrimdışı bir şekilde okuyorsanız bana eposta ile veya telefonla ulaşın, size bir çözüm bulmaya çalışalım.

Sağlıklı günler diliyorum.