açık anahtar şifreleme sistemini öğrenmek için aşağıdaki soruları, gerekiyorsa program, veya kağıt üstünde gösteriniz.

1. Bazı işlemleri tek yönlü yapmak kolay ama tersini alması çok zordur. Örneğin boyayı karıştırınca geri döndüremezsiniz. Yada çarpma işleminin tersi zor diye derste bahsetmiştik. Aklınıza gelen 1 tane yaratıcı, bilgisayar üstünde tek yönlü hızlı, tersi çok zor olan birşey düşünüp bir kaç cümle ile kriptolojide nasıl kullanılabileceğini yazınız.

2. 9 basamaklı 2 büyük asal sayı seçin. (Eğer bölme işleminin hesaplanması 5 dakikadan fazla sürüyorsa basamak sayısını küçültebilir yada 1 dakikanın altındaysa büyütebilirsiniz) bu sayıları önce çarpan, sonra çarpanlarına ayıran kod yazın. çarpanlarına ayırma algoritmasını düşünüp kendiniz tasarlayacaksınız, internetten fikirlere bakabilirsiniz. çalıştırın ve öncesine sonrasına timestamp koyup, geçen zamanı ölçüp kaydedin raporlayın. programlama dili serbest, kodlara sunum şeklinde de anlattıracağım, kendiniz yazın. bir kaç cümle ile ne öğrendiğinizi ve süreleri yazın, kodu da ekleyin.

3. RSA sisteminin nasıl hesaplandığını gördünüz, p q, e değerlerini 2 şer basamaklı sayılar şeklinde konsoldan yada ekrandan girdirtip, ardından verilen bir sayıyı önce şifreleyen, ardından çözen, ve bu süreçte işlemleri yaparken bütün değerleri, hesaplamaları vs. satır satır açıklama şeklinde konsola yada ekrana yazan bir program oluşturun. çalıştırıp ekranlarını yazın. (bu işlemler sınavda gelecek büyük ihtimal haberiniz olsun) . Sistem hata kontrolü yapıyorsa ekstra puan vereceğim, örneğin e değeri p-1*q-1 den fazla olamaz vs. gibi , bu tarz kontrolleri eklediyseniz ayrıca yazın.

programlama içerdiği için , zor gibi gözükebilir ödevler. kriptoloji dünyasını öğrenmeniz için önemli. kolay gelsin. sorularınızı mümkünse whatsapp üstünden yazarsınız, telefon numaram sizlerde var, daha kolay geri dönüş sağlarım