AYRIK MATEMATIK FINAL SORULARI (A GRUBU)

Soru 1.



Aşağıda verilen kurallara göre Ege bölgesi haritasını graph kullanarak renklendirmeniz gerekmektedir.

|  |  |
| --- | --- |
| Renk | 1 şehir  için tutar |
| Kırmızı | $100 |
| Mavi | $200 |
| Yeşil | $300 |
| Siyah | $400 |
| Sarı | $500 |

1. İki komşu şehir aynı renkte olmayacak.
2. Kullandığınız her rengin her kullanımı için bir fiyatı var.
3. En ucuz şekilde boyamanız gerekir.

Her renk için tutarlar tabloda verilmiştir   
**(İpucu: Önce Graph oluşturun, derecesi en büyük düğümden başlayarak renklendirme yapınız. (30P)**

**Soru 2.**

**RSA Algoritması**

**Step 1. Anahtar Üretimi**

1. İki asal sayı seçiniz (p ve q)

2. n=p\*q hesaplayınız

3. φ(n) = (p - 1) \* (q - 1) hesaplayınız

4. Bir e sayısı seçiniz öyle ki obeb(φ(n),e)=1 dir

5. Bir d sayısı bulunuz öyle ki d\*e mod φ(n) = 1 dir.

6. Açık anahtar: (e, n)

7. Gizli anahtar: (d, n)

**Step 2. Şifreleme**

Bir m mesajının şifrelenmiş hali: ile hesaplanır.

**Step 3. Deşifreleme**

Bir c şifreli mesajının orjinal hali: ile hesaplanır.

Yukarıdaki RSA algoritmasını kullanarak, m=6 yi önce şifreleyip daha sonra deşifre ediniz. **(20P)**

**(İpucu: p ve q asal sayılarını küçük seçmeniz işlem kolaylığı sağlayacaktır.)**

**Soru 3.** Dört kişi “GOOD NIGHT FRIENDS” ifadesini aşağıdakine göre şifreliyor:

1. person: G O O D N I G H T

F R I E N D S X X

1. person:

GF

OR

OI

DE

NN

ID

GS

HX

TX

1. person:

GFOROI

DENNID  
 GSHXTX

1. person: GFOROIDENNIDGSHXTX
2. Buna göre şifrelenen aşağıdakl ifadeyi çözünüz: “YDOMUYADREEAGROXOX”
3. Nasıl yapıldığını kısaca anlatınız.   
   (**20P**)

**Soru 4.** Simetrik (tek anahtarlı) ve Asimetrik (çift anahtarlı) şifreleme nasıl gerçekleştirilir, izah ediniz? Aralarındaki farkları anlatınız. **(20P)**

**Soru 5.** Çelişki ile ispat yöntemini kullanarak gösteriniz ki

eşitliğini sağlayan bir r rasyonal sayısı yoktur. **(20P)**

**[İpucu: Varsayın ki rasyonel ve şeklinde bir kök olsun, burada a ve b tamsayı ve a/b en sade formdadır. obeb(a,b)=1. nin a ve b ye bağlı eşitligini kullanarak tamsayılardan oluşan bir denklem elde edin ve bu denklemde a ve b nin teklik ve çiftlik durumlarını inceleyin.]**