Ad Soyad:
Numara:
Süre: 75 dakika

1Q	2Q	3Q	4Q	5Q	Toplam

AYRIK MATEMATIK BÜTÜNLEME SORULARI (A GRUBU)

Soru 1. a) Herhangi bir pozitif n tamsayısı için, gösteriniz ki n çifttir ancak ve ancak 7n + 4 çifttir. (**15P**)
İpucu: A ⇔ B ≡ **(**A⟹B) ∧ (B ⟹ A)

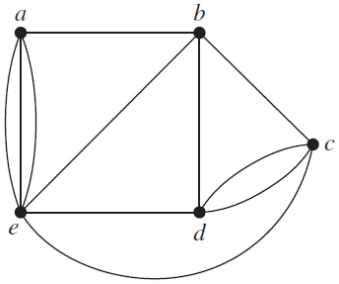
Soru 1. b) Herhangi bir pozitif n tamsayı için,

$$1 \times 1! + 2 \times 2! + \cdots + n \times n! = (n + 1)! - 1$$

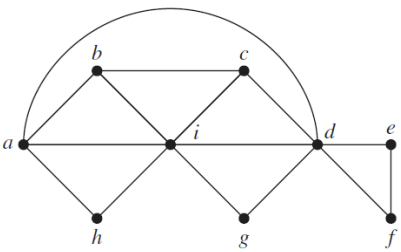
önermesinin doğruluğunu Tümeavrım yöntemini kullanarak bulunuz. (**15P**)

Soru 2. a) Aşağıda verilen grafların bir Euler devresine sahip olup olmadığını belirleyin. Varsa böyle bir devre oluşturun. Euler devresi yoksa, grafın bir Euler yoluna sahip olup olmadığını belirleyin ve varsa böyle bir yol oluşturun. **(10P)**

(I)

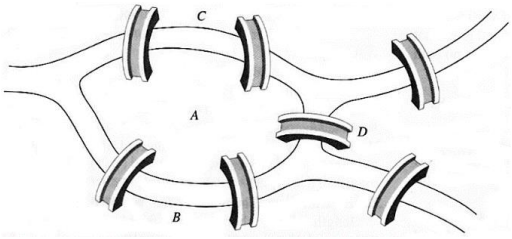


(II)

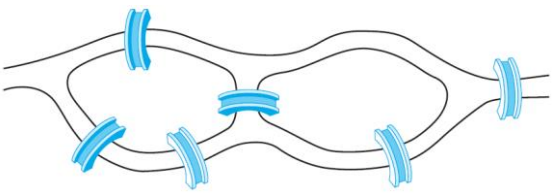


Soru 2. b) Aşağıdaki şekillerde gösterilen nehire kurulan köprülerin her biri yalnızca bir kez geçilip başlangıç noktasına geri dönülebilir mi? Nasıl ve neden? (İpucu: Verilen haritalar için bir graf oluşturunuz) **(10P)**

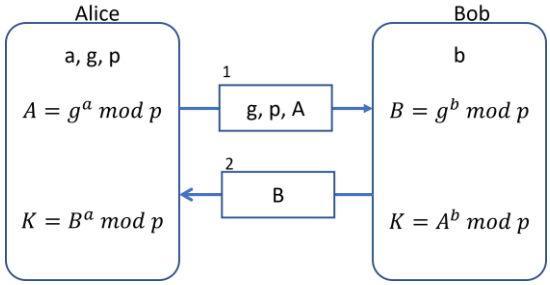
(III)



(IV)



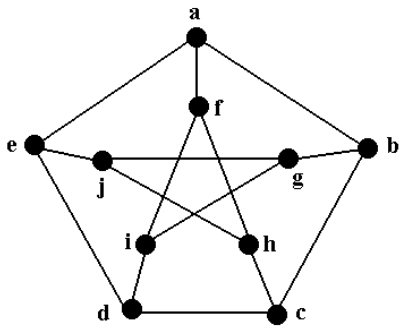
Soru 3. Yandaki resimde, 2 kişinin Diffie-Helmann anahtar değişim algoritmasını kullanarak nasıl bir ortak anahtar oluşturabileceği gösterilmiştir. Alice ve Bob aralarında anlaşıp **p=11 (asal)** ve taban olarak **g =5** seçerler. Alice gizli bir **a=4** sayısı seçer ve Bob'a **g, p** ve hesapladığı **A**'yı gönderir. Bob gizli bir **b=6** sayısı seçip **B**'yi hesaplayıp Alice'e gönderir.



Verilenlere göre, Alice, Bob un Diffie-Helmann anahtar değişim algoritmasını kullanarak bir ortak anahtar oluşturmalarını sağlayınız. **(15P)**

Cevap:

Soru 4. Aşağıdaki grafı, graf boyama algoritmasını kullanarak renklendirmek istiyoruz. En az kaç renk kullanarak bu iş yapılabilir? **(15P)**



Cevap:

Soru 5. MD5 hashing fonksiyonu herhangi bir boyuttaki giriş dizisinden 128 bitlik bir binary (32 bitlik hexadecimal) bir sonuç (özet) üretir. Örneğin,

MD5("The quick brown fox jumps over the lazy dog")= 9e107d9d372bb6826bd81d3542a419d6 ,

MD5(1234) = 81dc9bdb52d04dc20036dbd8313ed055

Buna göre;

a) 128 bitlik binary sonuç için kaç tane farklı alternatif sonuç üretilebilir? **(10P)**
b) En az kaç tane farklı giriş dizisini MD5 ile hash fonksiyonuna maruz bırakırsak, farklı iki karakter dizisinin hash değerleri aynı olur? Neden? (Güvercin yuvası prensibinden faydalanınız) **(10P)**

Cevap: