Ad Soyad:
Numara:
Süre: 75 dakika

1Q	2Q	3Q	4Q	5Q	Toplam

AYRIK MATEMATIK FINAL SORULARI (A GRUBU)

Q1. Birbirini takip eden 0'lardan veya 1'lerden oluşan bloklara ***run*** denir. 0 ve 1 lerden oluşan akan bir şifrenin rastgele oluşturulup-oluşturulmadığını run testi ile aşağıdaki gibi test edebiliriz:

- n bitlik bir dizide toplam $(n+1)/2$ tane run olması beklenir;
- Uzunluğu 1 olan runların sayısının $(n+1)/2^2$ olması beklenir
  …
- Uzunluğu k olan runların sayısının $(n+1)/2^{k+1}$ olması beklenir.

Örneğin, $\mathbf{z = 1101000}$ akan şifresi için $\boldsymbol{n = 7}$, beklenen run sayısı 4 tür. Ayrıca
- Uzunluğu 1 olan run sayısı: $\boldsymbol{(n+1)/2^2 = 2}$ dir.
- Uzunluğu 2 olan run sayısı: $\boldsymbol{(n+1)/2^3 = 1}$ dir.
- Uzunluğu 3 olan run sayısı: $\boldsymbol{(n+1)/2^4 = 0.5} \cong 1$ dir.

Gerçekten de, bu akan şifre için 4 run aşağıdaki gibi elde edilir;
- Uzunluğu 1 olan runlar: 0 ve 1 (2 tane)
- Uzunluğu 2 olan run; 11 (1 tane)
- Uzunluğu 3 olan run; 000 (1 tane)

Buna göre, 15-bit uzunluğunda run testini geçen bir akan şifre oluşturunuz.

Cevap:

Q.2 A ve B şahısları için El Gamal açık anahtar şifreleme algoritması aşağıda belirtilmiştir.

Anahtar Oluşturma (A şahsı)
- p asal sayısını ve Z_p^* kümesini üreten bir α ilkel kökünü seçer.
- $1 \le a \le p-2$ eşitsizliğini sağlayan bir a gizli anahtarını seçer ve $\alpha^a \text{modp}$ değerini hesaplar.
- A nın açık anahtarı $\{p, \alpha, \alpha^a \text{modp}\}$ nı, B şahsına iletir.

Şifreleme (B şahsı)
- $0 \le m \le p-1$ eşitsizliğini sağlayan bir m tamsayısını mesaj olarak seçer.
- $1 \le b \le p-2$ eşitsizliğini sağlayan bir b gizli anahtarını seçer ve $\gamma = \alpha^b \text{modp}$ değerini ve $\delta = m(\alpha^a)^b \text{modp}$ hesaplar.
- $c = \{\gamma, \delta\}$ kapalı metnini, A şahsına iletir.

Deşifreleme (A şahsı)
- $\gamma^{-a} \text{modp}$ değerini hesaplar ve $\gamma^{-a}.\delta \,\text{modp}$ değerini hesaplayarak m yi bulur.
  İpucu: $\gamma^{-a} \text{modp} = \gamma^{p-1-a} \text{modp}$

A şahsı $p = 11$ ve $\alpha = 2$ üretecini (ilkel kökünü) ve kendine gizli anahtar olarak $a = 6$ sayısını seçsin. B şahsı da, kendine gizli anahtar olarak $b = 3$ sayısını seçsin. Buna göre, **B'nin A'ya, $\boldsymbol{m = 7}$ mesajını göndermesini ve A'nın bu mesajı okumasını sağlayınız.**

Cevap:

Q3. Aşağıdaki şifreleme işleminde Türkçe alfabeden istifade edilmiştir.

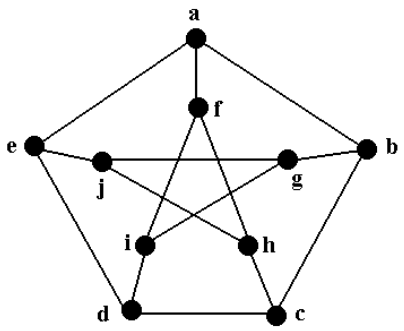
A B C Ç D E F G Ğ H I İ J K L M N O Ö P R S Ş T U Ü V Y Z

Düz Metin	**Şifreli Metin**
TÜRKİYE	UYTONDJ
???	CCBUEP

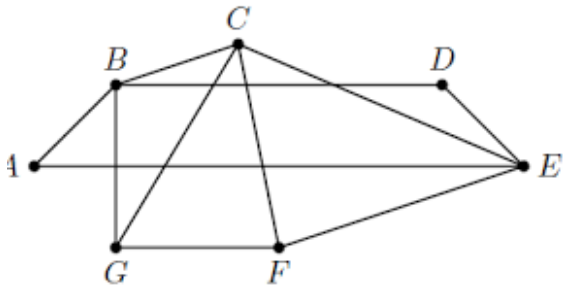
Buna göre CCBUEP şifreli metnine karşılık gelen düz metni bulunuz.

Cevap:

Q4.a Aşağıdaki grafiğin bir Hamilton Grafiği olup olmadığını gösterin. (Bir devre inşa et)



Q4.b Aşağıdaki grafiğin bir Euler Grafı olmadığını fakat bir Euler yoluna sahip olduğunu sebebini belirterek gösterin. (Bir yol inşa et)



<u>Q5.</u> Asimetrik kriptografi nedir? Çalışma prensibini, avantajlarını ve dezavantajlarını açıklayınız. Simetrik kriptografiden farkı nedir?

Cevap: