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:

* bitlik bir dizide toplam tane run olması beklenir;
* Uzunluğu olan runların sayısının olması beklenir

…

* Uzunluğu olan runların sayısının

olması beklenir.

Örneğin, akan şifresi için , beklenen run sayısı 4 tür. Ayrıca

- Uzunluğu 1 olan run sayısı: dir.

- Uzunluğu 2 olan run sayısı: dir.

- Uzunluğu 3 olan run sayısı: 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:***

***Cevap:***

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

**Anahtar Oluşturma (A şahsı)**

* asal sayısını ve kümesini üreten bir ilkel kökünü seçer.
* eşitsizliğini sağlayan bir gizli anahtarını seçer ve değerini hesaplar.
* nın açık anahtarı nı, B şahsına iletir.

**Şifreleme (B şahsı)**

* eşitsizliğini sağlayan bir tamsayısını mesaj olarak seçer.
* eşitsizliğini sağlayan bir gizli anahtarını seçer ve değerini ve hesaplar.
* kapalı metnini, A şahsına iletir.

**Deşifreleme (A şahsı)**

* değerini hesaplar ve değerini hesaplayarak yi bulur.

İpucu:

A şahsı ve üretecini (ilkel kökünü) ve kendine gizli anahtar olarak sayısını seçsin. B şahsı da, kendine gizli anahtar olarak sayısını seçsin. Buna göre, **B’nin A’ya, mesajını göndermesini ve A’nın bu mesajı okumasını sağlayınız.**

***Cevap:***

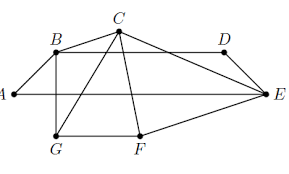
***Q3.*** Aşağıdaki şifreleme işleminde Türkçe alfabeden istifade edilmiştir.

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

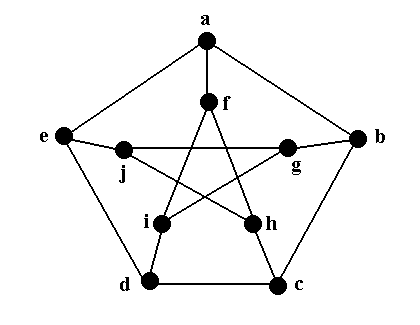
|  |  |
| --- | --- |
| **Düz Metin** | **Şifreli Metin** |
| TÜRKİYE | UYTONDJ |
| ??? | CCBUEP |
|  |  |

Buna göre CCBUEP şifreli metnine karşılık gelen düz metni bulunuz.

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



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



***Cevap:***

**Q5.** Asimetrik kriptografi nedir? Çalışma prensibini, avantajlarını ve dezavantajlarını açıklayınız. Simetrik kriptografiden farkı nedir?