CENG 122
Nesneye Yönelik Programlama Laboratuvarı
Hafta 3

11 Mart 2024

1 AMAÇ

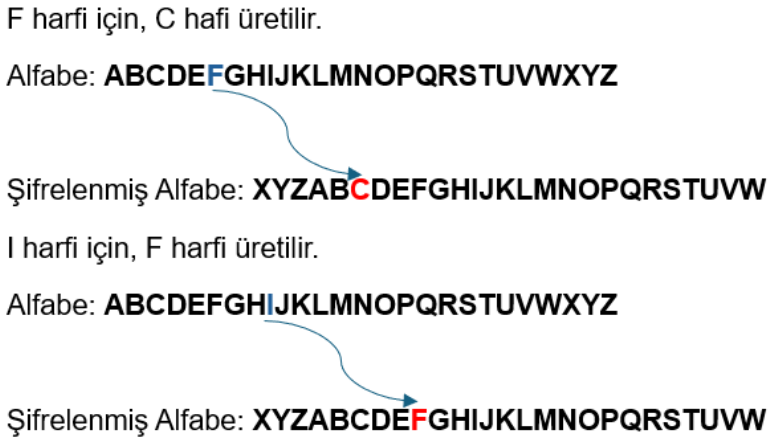
a. String işlemleri

b. Caesar Cipher decryption

c. Vigenere Cipher implementasyonu

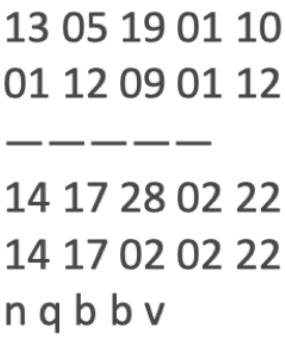
2 YAPILACAKLAR

- Sezar şifreleme algoritması, oldukça yaygın kullanılan şifreleme algoritmalarından bir tanesidir. Şifreleme yapılırken, key bilgisine göre; şifrelenmiş alfabeye ihtiyaç duyulmaktadır. İlk önce key bilgisine göre; şifrelenmiş alfabe oluşturulur. Sonrasında ise; her harf için, şifrelenmiş harf bilgisi üretilir. Tüm bu verilen bilgilere göre; şifreleyen encryption algoritmasını oluşturunuz. (Örneğin, key=3 için; "FIRST" kelimesine ait ilk iki harfin şifrelenmesi aşağıda verilmiştir.)



- Sezar şifreleme algoritmasına göre; şifrelenmiş bir mesajın içeriğini gösteren decryption algoritmasını oluşturunuz.

- Vigenere şifreleme, ilkel şifreleme yöntemlerinden birisidir. Kaydırma Şifrelemesi ve yerine koyma şifrelemesi gibi şifrelemelerden en önemli farkı şifrenin her harfe aynı şekilde değil bir harf bloguna uygulanmasıdır. Örnek olarak "MESAJ" kelimesini "ALI" şifresi ile şifrelemek isteyelim bu durumda:
  MESAJ : 13 5 19 1 10
  ALI : 1 12 9 karşılıklarına sahiptir. Şifreleme işlemi aşağıdaki gibi gerçekleşmektedir.



Açan taraf şifrelemenin tersini yani sırasıyla harflerden anahtarı çıkararak metni bulabilir.
Bu labda StringBuilder ve String kullanarak dışarıdan girilen bir metin ve anahtara göre Vigenere şifreleme yöntemine göre oluşan şifreli metini gösteren Java programını yazınız.