

CENG 122

Nesneye Yönelik Programlama Laboratuvarı

LAB 3

11 Mart 2021

1 AMAÇ

- String işlemleri
- Caesar Cipher decryption
- Vigenere Cipher implementasyonu

2 YAPILACAKLAR

- Sezar şifreleme algoritması, oldukça yaygın kullanılan şifreleme algoritmalarından bir tanesidir. Buna göre verilen key bilgisine 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 metni gösteren Java programını yazınız.

```
13 05 19 01 10
01 12 09 01 12
-----
14 17 28 02 22
14 17 02 02 22
n q b b v
```