

**AMAÇ :** Bu uygulamanın amacı kişiye ortadaki adam saldırısının genel çalışma prensibine dair bilgi vermek ve kişinin anahtar oluşturma kümesi küçük anahtar kümeleri için ortadaki adam saldırı sistemi oluşturabilmesine katkıda bulunmaktır.

## **ÖNBİLGİ :**

**Ortakdaki Adam Saldırıları :** Ortadaki adam saldırı genel olarak İki kişi arasında veri iletimi gerçekleştiği esnada üçüncü bir kişinin kendini gizleyerek veri iletimine müdahale ederek verinin elde edilmesi, değiştirilmesine denir.

## **UYGULAMA :**

### **A. Uygulama Öncesi yapılacaklar :**

Brute-force\_deşifreleme (şifreli\_mesaj)

Ortakdaki adam saldırısı için şifrelenmiş veriyi deşifrelemek için brute-force saldırısı gerçekleştirecek brute-force\_deşifreleme algoritmasını tasarlayıp kodlayınız.

### **B. Uygulamanın Yapılışı:**

Şifreleme Sistemi 1 :  $f(x) = \text{key} * x \bmod 26$ , where  $\text{gcd}(\text{key}, 26) = 1$  (Muhtemel anahtar sayısı 12)

Şifreleme Sistemi 2 :  $g(x) = (\text{key} + x) \bmod 26$  (Muhtemel anahtar sayısı 26)

Bu iki şifreleme sistemi ile oluşturulmuş metinlere brute-force\_deşifreleme fonksiyonu ile ortakdaki adam saldırı düzenleyip, deşifreleme işlemi gerçekleştirip, anahtar değerini elde ediniz ve bu anahtarı kullanarak içeriği değiştirilmiş yeni mesaj yayınlayınız.

## **ANALİZ :**

- Deşifreleme işlemi ne kadar sürmüştür?
- Mod değerini artırıp muhtemel anahtar sayısı değiştiğinde, saldırı süresi ne kadardır?
- Sisteminiz için mod eşik değeri nedir?