LİNEER KRİPTANALİZ DENEY SORULARI

1. Şekil 3 deki S-BOX için aşağıdaki girişler verildiğinde çıkışı ne olur belirleyiniz.
    a. 110100
    b. 011011
    c. 110111
    d. 001110
2. SBox'ın bu deneyden anlatılan kripto sistemdeki görevi nedir? Neden kullanılmıştır.
3. Linear Kripto analiz yönteminin başarısı nelere bağlıdır.
4. Denklem 2 nin elde edilmesi için gerekli ara işlemleri yapınız
5. Pilling up Lemma yı ispat ediniz. 3 ve 4 giriş için ispat etmeniz yeterlidir.