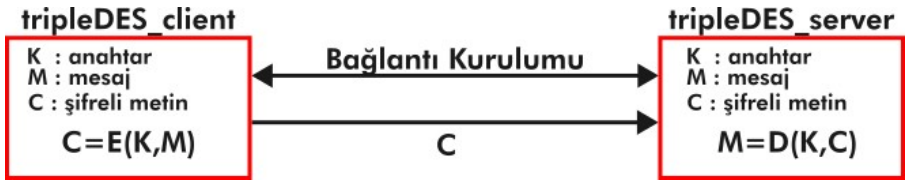
ÖDEV 1 : TripleDES ve AES Simetrik Şifreleme Algoritmalarının Uygulanması

Son Ödev Gönderim Tarihi	10 Mart 2025 Pazartesi 23.59
Sunum Tarihi	11 Mart 2025 Salı 12.00-13.15
Sunum Yeri	EA 105

TripleDES ALGORİTMASININ UYGULANMASI

TripleDES algoritmasını kullanarak lokal bir proses üzerinde anahtar üretme, şifreleme ve çifre çözme işlemlerini gerçekleştiren **tripleDES.py** dosyası sizinle paylaşılmıştır. Bu dosyadaki kodları inceleyiniz. Bu kodlardan faydalanarak, yerel ağa bağlı iki cihaz arasında şifreli mesajın iletildiği bir istemci sunucu uygulamasına dönüştürünüz. İstemci ve sunucu cihazları arasındaki bağlantı kurulduktan sonra, istemci taraf bir düz metni K anahtarı ile şifreleyerek sunucu cihaza gönderecektir. Sunucu ise aldığı şifreli metni yine K anahtarını kullanarak şifre çözecek ve düz metni elde edecektir. Anahtarı bir defa ürettikten sonra bir değişken olarak saklayabilirsiniz. İki adet dosyayı **tripleDES_server_ogrenciNo.py** ve **tripleDES_client_ogrenciNo.py** dosyalarını Microsoft Teams üzerinden sisteme yüklemeniz gerekmektedir. Sunucu ve istemci arasındaki haberleşme için paket tercihi size bırakılmıştır.



AES ALGORİTMASININ UYGULANMASI

Benzer şekilde, AES algoritmasını kullanarak lokal bir proses üzerinde anahtar üretme, şifreleme ve çifre çözme işlemlerini gerçekleştiren **aes.py** dosyası sizinle paylaşılmıştır. Bu dosyadaki kodları inceleyiniz. Bu kodlardan faydalanarak, yerel ağa bağlı iki cihaz arasında şifreli mesajın iletildiği bir istemci sunucu uygulamasına dönüştürünüz. İstemci ve sunucu cihazları arasındaki bağlantı kurulduktan sonra, istemci taraf bir düz metni K anahtarı ile şifreleyerek sunucu cihaza gönderecektir. Sunucu ise aldığı şifreli metni yine K anahtarını kullanarak şifre çözecek ve düz metni elde edecektir. Anahtarı bir defa ürettikten sonra bir değişken olarak saklayabilirsiniz. İki adet dosyayı **aes_server_ogrenciNo.py** ve **aes_client_ogrenciNo.py** dosyalarını Microsoft Teams üzerinden sisteme yüklemeniz gerekmektedir. Sunucu ve istemci arasındaki haberleşme için paket tercihi size bırakılmıştır.