

ÖDEV

DERSİN ADI : KRİPTOGRAFİ VE BİLGİSAYAR GÜVENLİĞİ
DERSİN KODU : BİL 470
DERSİN SAAT VE KREDİSİ : (3+0=3)
TESLİM TARİHİ : 08.01.2021 17:30)

Araştırma: • OSI temel referans modelinin uygulama katmanında (katman 7), ağ katmanında (katman 3) ve taşıma katmanında (katman 4) kriptografik protokollerin uygulanmasının görelî avantajları ve dezavantajlarını araştırarak örneklerle karşılaştırmalı olarak açıklayın. .

Programlama projesi: : C veya python ile gerçekleştirilecek olan bu araçta şifreleme/deşifreleme ve Özütleme, dosya bütünlüğünün denetimi yöntemleri bizzat gerçekleştirilecek olup, arşiv/API kullanılmayacaktır. Gerçekleştirilen Programların kaynak kodları açıklamalı olarak verilecektir;

- AES şifreleme algoritmasının gerçekleştirilmesi ve şifreleme/deşifrelemede kullanılması(test verileri ile birlikte).
- Gerçekleştirilen Şifreli şifreleme algoritması kullanılarak CBC ve OFB modlarında çalışmayı gerçekleştirip testlerini yapacak şekilde getiriniz.
- Herhangi bir doküman (.doc/.docx, .pdf, ppt, xls vs) üzerinde değişiklik yapıp yapılmadığını ve yapının kimliğini anlamak için, özetini alacak ve sadece işlem yapan kişinin bildiği bir anahtar ile şifreleyip dosyanın sonuna ekleyecek bir araç (b şikkındaki gerçekleştirilecek özet fonk. Olarak kullanınız)
- Dosyanın bütünlüğünün değişip değişmediğinin kontrolü için, c)deki işlemleri yaparak ilk üretilen özet değeri ile karşılaştıran doğrulama aracını gerçekleştirip örnek testleri gösteriniz.

Ödev problemlerinde yapılan çalışma sonuçları yazılı rapor halinde .doc/docx olarak verilen bitirme zamanından önce teams'deki ders grubuna yüklenecektir.

Başarılar. Dilerim.