ÖDEV

DERSİN ADI : KRİPTOGRAFİ VE BİLGİSAYAR GÜVENLİĞİ
DERSİN KODU : BİL 470
DERSİN SAAT VE KREDİSİ : (3+0=3)
TESLİM TARİHİ : 31.12.2021 17:30)

Araştırma: • Hafif siklet(lightweight) simetrik şifreleme algoritmaları ve yeni önerilen algotirmaların analizi ve karşılaştırmalı olarak açıklayın. (BIL470-liste-konu, Verilen listede belirtilen iki adet kriptogtrafi algoritması için). https://csrc.nist.gov/Projects/lightweight-cryptography/email-list bu bağlantıdaki bilgiler kullanılacak

.

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

a) İncelenen iki adet hafif siklet şifreleme algoritmalarının gerçeklenmesi ve şifreleme/ deşifrelemede kullanılması(test verileri ile birlikte).
b) Gerçeklenen Şimetrik şifreleme algoritması kullanılarak CBC ve OFB modlarında çalışmayı gerçekleyip testlerini yapacak şekle getiriniz.
c) Herhangi bir doküman (.doc/.docx, .pdf, ppt, xls vs) üzerinde değişiklik yapılıp yapılmadığını ve yapanın kimliğini anlamak için, özütünü alacak ve sadece işlem yapan kişinin bildiği bir anahtar ile şifreleyip dosyanın sonuna ekleyecek bir araç (b şıkkındaki gerçeklemeyi özüt fonk. Olarak kullanınız)
d) Dosyanın bütünlüğünün değişip değişmediğinin kontrolü için, c)deki işlemleri yaparak ilk üretilen özüt değer ile karşılaştıran doğrulama aracını gerçekleyerek 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.