SAKARYA ÜNİVERSİTESİ SİBER GÜVENLİK YL. 2022-2023 BAHAR YARIYILI KRİPTOLOJİYE GİRİŞ DERSİ PROJE DÖKÜMANI

PROJE İLE İLGİLİ AÇIKLAMALAR

- Proje kapsamında **yeni bir blok şifreleme algoritması tasarımı ve kodlaması** yapılarak, şifreleme ve şifre çözme işlemleri gerçekleştirilecektir.
- İki kişilik gruplar halinde projeyi yapabilirsiniz.
- Şifreleme işlemlerinde text, resim, ses vb. veriler kullanılabilir.
- Kodlama işleminde herhangi bir programlama dili tercih edilebilir.
- Ödev teslimi Sabis'te açılacak olan ödev teslim modülü üzerinden yapılacaktır. Teslim tarihinden sonra sisteme yüklenen ödevler kabul edilmeyecektir.
- Projede **şifrelenecek olan veri, kullanılacak anahtarlar** kullanıcıdan alınmalı, **şifreleme ve çözme işlemi sonucu elde edilen sonuçlar** geliştirilecek ara yüzde gösterilmelidir.
- Şifreleme algoritması tasarımda dikkat edilecek hususlar:
  - Geliştireceğiniz şifreleme algoritmasının blok diyagramı çizilerek çalışması raporda detaylı bir şekilde açıklanacaktır.
  - Feistel veya SPN mimarisinde tasarım yapabilirsiniz.
  - Algoritma blok boyutu, anahtar boyutu ve döngü adetini siz belirlemelisiniz.
  - Algoritma tasarımında derste anlatılmış olan karıştırma ve yayılma özelliklerini sağlayacak (SBOX-Permütasyon- Satır sütün işlemleri) bileşenleri kullanabilirsiniz.
  - Tasarım sırasında literatürdeki var olan algoritmaları inceleyebilirsiniz fakat tasarımınızın özgün olması gerekmektedir.
  - Döngü anahtarlarının üretimi için basit bir anahtar genişletme algoritmasını da tasarımınız içermelidir.
  - Son olarak tasarladığınız algoritmanın şifreleme ve çözme işlemlerini doğru olarak gerçekleştirdiğini kontrol ettikten sonra, performansını incelemelisiniz. Elde edilen performans sonuçlarına göre tasarımınızda değişiklik yapabilirsiniz. (Örnek olarak 1 mb. veriyi kaç sn'de şifreleyip çözdüğünü sonuç olarak sunabilirsiniz.)

ÖDEV İÇERİĞİ:

- Proje kaynak kod dosyaları (header-source file)
- Proje açıklama dosyası (readme)
- Program çalıştırılabilir dosyası (*.exe)
- Proje ödev dökümanı (içeriği aşağıdaki gibi düzenlenecektir.)
  * Kapak sayfası
  * Geliştirilen şifreleme algoritmasına ait bilgilendirme dökümanı (kodları buraya yapıştırmayın)
  *Uygulamanın örnek çalıştırma ekran çıktıları
  * Performans sonuçları

Projenin sisteme yüklenmesi: Ödev içeriğinde yer alan tüm dokümanları tek bir klasöre (klasörün ismi öğrenci numaranız olmalı) kopyalayarak, sıkıştırdıktan sonra tek bir parça halinde yüklemeniz gerekmektedir. (y221210095-y221210024.rar)

Değerlendirme ile ilgili uyarılar: Bu ödevin amacı, bir şifreleme algoritmasının tasarım, kodlama ve uygulamasının gerçekleştirilmesini sağlamaktır. Bu sebeple internet üzerinden bulacağınız hazır kodlar veya arkadaşlarınızın kodlarını projenizde kullanmamalısınız.

Proje son teslim tarihi: 26.05.2023