SAKARYA ÜNİVERSİTESİ BİLGİSAYAR MÜHENSİLİĞİ 2023-2024 GÜZ YARIYILI
KRİPTOLOJİYE GİRİŞ DERSİ PROJE DÖKÜMANI

Şifreleme Algoritması Tasarımı Projesi

Proje Tanımı:

Bu proje, güvenli iletişim ve veri koruma amaçlarıyla kullanılmak üzere yeni bir şifreleme algoritması tasarlamayı amaçlamaktadır. Proje, temel şifreleme prensiplerini kullanarak bir blok şifreleme algoritması tasarımı ve performans ölçümleri üzerine odaklanacaktır. Literatürdeki algoritmalardan esinlenerek yeni bir algoritma tasarımı yapılması beklenmektedir.

Amaç:

- Yüksek güvenlik seviyelerine ulaşabilecek bir şifreleme algoritması tasarlamak.
- Anahtar üretimini güvenli bir şekilde gerçekleştirmek.
- Geliştirilen algoritmanın kodlamasını yapmak.
- Performans ölçümleri yaparak algoritmanın etkinliğini değerlendirmek.

PROJE İLE İLGİLİ AÇIKLAMALAR

- Proje kapsamında bir şifreleme algoritması tasarımı, kodlaması ve analizi yapılarak, şifreleme ve şifre çözme işlemleri gerçekleştirilecektir.
- Üç 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.
- Github üzerinden kayıt oluşturulmayan projeler değerlendirilmeyecektir.

Proje Adımları ve Raporlama:

Proje aşağıdaki adımları içermelidir ve raporlama bu içeriğe göre yapılacaktır.

Literatür Taraması:

Şu anda kullanılan popüler şifreleme algoritmalarını inceleyin. Mevcut zayıflıkları ve avantajları anlamak için literatür taraması yapın ve bunları raporlayın.

Temel Prensiplerin Belirlenmesi:

Şifreleme için temel prensipleri belirleyin (örneğin, simetrik veya akış şifreleme/ şifreleme mimarisi/ blok boyutu/anahtar boyutu/ döngü sayısı vb.).

Algoritma Tasarımı:

Temel prensiplere dayalı olarak şifreleme algoritmanızın tasarımını yapın. Algoritmanın anahtar uzunluğu, blok boyutu gibi önemli parametreleri belirleyin. Algoritma ve anahtar üretimini bir blok diyagram üzerinden açıklayınız.

Anahtar Üretimi:

Güvenli anahtar üretimi sağlayacak bir yapı tasarlanacak ve döngüler için üretim adımları açıklanacaktır.

Algoritmanın Kodlanması:

Tasarladığınız algoritmayı seçeceğiniz bir program dilini kullanarak kodlayınız. Projede şifrelenecek olan veri, kullanılacak anahtarlar kullanıcıdan alınmalı, şifreleme ve çözme işlemi sonucu elde edilen sonuçlar geliştirilecek ara yüzde gösterilmelidir. Aşağıdaki dosyalar hazırlanacak rapor dosyası ile birlikte sisteme yüklenecektir.

- Proje kaynak kod dosyaları (header-source file)
- Proje açıklama dosyası (readme)
- Program çalıştırılabilir dosyası (*.exe)

Performans Ölçümleri:

Tasarlanan algoritmanın performansını değerlendirmek için gerekli testleri belirleyin. Hız, bellek tüketimi ve diğer performans metriklerini ölçün.

Raporlama:

Proje sonuçlarını içeren bir rapor hazırlayın. Algoritmanın ürettiği çıktılara ait ekran alıntılarını lütfen proje raporuna ekleyiniz.

****

Projenin geliştirilmesi ve teslimi:

Projenin geliştirilmesi aşamasında proje ekibinden bir kişi https://github.com/ üzerinde proje için bir kayıt oluşturacak ve geliştirme işlemleri bu adres üzerinden yürütülecektir. Sonuç raporuna bu adres eklenecektir.

Sisteme yüklenmesi: Ödev içeriğinde yer alan tüm dokümanları (proje kodları, rapor dosyası) tek bir klasöre (klasörün ismi öğrenci numaranız olmalı) kopyalayarak, sıkıştırdıktan sonra tek bir parça halinde sisteme yüklenecektir. (b211210095_b221210024_ b201210081.rar/zip)

Değerlendirme ile ilgili uyarılar: Bu ödevin amacı, bir şifreleme algoritmasının tasarımı, kodlama ve uygulamasının gerçekleştirilmesini sağlamaktır. Bu sebeple internet üzerinden bulacağınız hazır kodlar veya arkadaşlarınızın kodlarını projenizde kullanmamalısınız. Yapılan kontrollerde böyle bir durumun tespiti halinde proje değerlendirmesinin sonucu sizi hiç mutlu etmeyecektir.

Proje son teslim tarihi: 30.12.2023 23:59