BLGM455 Bilgisayar Sistemleri ve Ağ Güvenliği

Lab 3 DES

Amaç: DES'in anlaşılması.

Görev

1. DES algoritmasını yazılım uygulaması olarak uygulayın.
2. Kullanılan belirli dönüşümlerin doğruluğunu kontrol ederek test edin:
   2.1. İlk Permütasyon
   2.2. İlk Permitason Tersi
   2.3. Genişleme/Permütasyon
   2.4. Tur (round) Anahtar Üretimi
      2.4.1. İzin Verilen Seçim 1
      2.4.2. Sol Dairesel Kaydırma Çizelgesi
      2.4.3. İzin Verilen Seçim 2
   2.5. Tur anahtarı ile XOR
   2.6. S-boxes (S-kutuları)
   2.7. S-boxes Sonrası Permütasyon P
   2.8. Sol Yarım ile olan XOR
   2.9. Yarımların Takası
3. Yapılan çalışmalar hakkında bir rapor hazırlayın.
   3.1. Kapak sayfası (Üniversite, Bölüm, Program, Ders, Laboratuvar Konusu, Takım Üyeleri, Öğretim Görevlisi, Laboratuvar Asistanı, Yıl, Sömestir, Şehir, Ülke)
   3.2. İçerik
   3.3. Problemin Tanımı
   3.4. Yapılan İş. Ele alınan 1, 2 numaralı problemler için, geliştirilen kodunuzu açıklayın. DES şifrelemeyi test değişkenlerini kullanarak hata ayıklayıcı adım modunda çalıştırarak ekran görüntülerini alıp çalışmanızı gösterin. Düz metin mesajın oluşturulmasını, şifrelenmesini, gönderilmesini, alınmasını, şifresinin çözülmesini, şifresi çözülen mesajın görüntülenmesini gösteren ekran görüntüleri sağlayın (düz metin mesajı ile aynı olacaktır)
   3.5. Sonuç
   3.6. Kaynaklar
   3.7. Kaynak Kodları İçeren Ek
   3.8. Lab ile ilgili arşivlenmiş (rar, zip vb.) tüm materyaller(kaynaklar, çalıştırılabilir dosyalar, test örnekleri, rapor)
4. **(Ek çalışma)** Ağ ortamında DES'in anlaşılması . DES algoritmasını, her biri mesaj oluşturma, şifreleme, gönderme, mesaj alma, şifre çözme ve görüntüleme işlemlerini yürüten iki bilgisayar kullanan dağıtılmış bir uygulama olarak uygulayın.
   4.1. Bir Mesaj Oluşturun, Şifreleyin ve Alıcı Prosesine Gönderin
   4.2. Gönderen Prosesen Bir Mesaj ALın, Şifresini Çözün ve Görüntüleyin
   4.3. Dağıtılmış sistemin ayarlarını tanımlayın (farklı makinelerde çalışan işlemlerin bağlantısını nasıl düzenlersiniz?)

Rapor ve uygulama Lab asistanı tarafından laboratuvar saatinde değerlendirilecektir.

Derecelendirme Politikası: Rapor –%50, Açıklamalar – %50