# **BLGM455 Güz 2019-2020**

# **Lab 3 İki Bilgisayarda DES**

**Alexander Chefranov tarafından 21 Mart 2019 tarihinde hazırlanmış olup Samed Reyhanlı tarafından 10 Aralık 2019 da Türkçe’ye çevrilmiştir.**

**Amaç:** Ağ ortamında DES'in anlaşılması.

**Görevler**

1. DES algoritmasını, her biri mesaj oluşturma, şifreleme, gönderme, mesaj alma, şifre çözme ve görüntüleme işlemlerini yürüten iki bilgisayar kullanan dağıtılmış bir uygulama olarak uygulayın.
2. Kullanılan belirli dönüşümlerin doğruluğunu kontrol ederek test edin:
	1. İlk Permütasyon
	2. İlk Permitason Tersi
	3. Genişleme/Permütasyon
	4. Tur (round) Anahtar Üretimi
		1. İzin Verilen Seçim 1
		2. Sol Dairesel Kaydırma Çizelgesi
		3. İzin Verilen Seçim 2
	5. Tur anahtarı ile XOR
	6. S-boxes (S-kutuları)
	7. S-boxes Sonrası Permütasyon P
	8. Sol Yarım ile olan XOR
	9. Yarımların Takası
	10. Bir Mesaj Oluşturun, Şifreleyin ve Alıcı Prosesine Gönderin
	11. Gönderen Prosesen Bir Mesaj ALın, Şifresini Çözün ve Görüntüleyin
3. Yapılan çalışmalar hakkında bir rapor hazırlayın ve yazdırın.
	1. Kapak sayfası (Üniversite, Bölüm, Program, Ders, Laboratuvar Konusu, Takım Üyeleri, Öğretim Görevlisi, Laboratuvar Asistanı, Yıl, Sömestir, Şehir, Ülke)
	2. İçerik
	3. Problemin Tanımı
	4. Yapılan İş
		1. 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)
		2. Dağıtılmış sistemin ayarlarını tanımlayın (farklı makinelerde çalışan işlemlerin bağlantısını nasıl düzenlersiniz?)
	5. Sonuç
	6. Kaynaklar
	7. Kaynak Kodları İçeren Ek
	8. Laboratuar ile ilgili tüm materyalleri içeren CD (kaynaklar, yürütülebilir dosyalar, test örnekleri, rapor)

**Rapor ve uygulama 25 Aralık 2019 Çarşamba günü Laboratuar Koordinatörü Samed Reyhanlı tarafından Lab 134’te laboratuvar saatinde (16:30) değerlendirilecektir.**

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