

**BLM 323**  
**BİLGİ GÜVENLİĞİ VE KRİPTOGRAFI**

Dr. Öğr. Üyesi Meltem KURT  
PEHLİVANOĞLU

# Ders Gün-Saati

- 1. Öğretim Pazartesi (13:00-15:50)
- 2.Öğretim Pazartesi (17:00-19:50)

# Dersin Amacı

Bu ders iki önemli çalışma alanının öğrenilmesini amaçlar.

1. Şifreleme
2. Güvenlik

Vize haftasına kadar;

- Matematiksel altyapı (Şifreleme için sonlu cisimler teorisi),
- Şifreleme algoritmalarının matematiksel altyapısının kapsamlı incelenmesi ve kodlanması,

Vize haftasından sonra;

- Kriptoanaliz teknikleri,
- Dijital imzalama yöntemleri konuları kapsamlı olarak işlenecektir.

Ders boyunca işlenecek konular birbiriyle bağlantılıdır, bu nedenle derse zamanında ve düzenli katılım önemlidir.

# Dersi Neden Almalıyım?

Bu ders, güvenlik alanının önemli bir çalışma konusu olan şifreleme bilimi hakkında kapsamlı bilgi verilmesini ve teorik bilgilerin uygulamaya aktarılmasını hedefler.

Dersi alacak öğrencilerin matematiksel alt yapı ve aktif kodlama yeteneğinin bir arada olması, dersin öğrenci açısından verimli geçmesini sağlayacaktır.

# Değerlendirme Ölçütü

- %40 Vize
- %60 Final

I. Bunun yanında, ders sırasında değerlendirme quizleri (**en az 2 değerlendirme quizi**)

Değerlendirme quizleri Vize/Final notlarınızı **önemli oranda (yapılacak quiz sayısına göre çarpan belirlenecektir)** etkileyecektir.

Değerlendirme quizleri içerikleri **yeni öğrendiğiniz konuyu veya önceki öğrendiğiniz konuları** kapsayabilir.

# Devamsızlık

- Derslerde yoklama alınacaktır.