# Ders Bilgi Formu

| Ders Adı | Kodu | Yerel Kredi | AKTS | Ders (saat/hafta) | Uygulama (saat/hafta) | Laboratuar (saat/hafta) |
|---|---|---|---|---|---|---|
| **Şifrelemeye Giriş** | MTM4532 | 3 | 6 | 3 | 0 | 0 |

| | |
|---|---|
| Önkoşullar | Yok |

| | |
|---|---|
| Yarıyıl | Bahar |

| | |
|---|---|
| Dersin Dili | İngilizce, Türkçe |
| Dersin Seviyesi | Lisans Seviyesi |
| Ders Kategorisi | Temel Meslek Dersleri |
| Dersin Veriliş Şekli | Yüz yüze |

| | |
|---|---|
| Dersi Sunan Akademik Birim | Matematik Mühendisliği Bölümü |
| Dersin Koordinatörü | Atanmamış |
| Dersi Veren(ler) | |
| Asistan(lar)ı | |

| | |
|---|---|
| Dersin Amacı | Sayılar teorisi bilgilerinin güncel hayata uygulanabilmesi. |
| Dersin İçeriği | Sayılar Teorisinde Bazı Temel Kavramlar ,Çarpanlara Ayırmanın Uygulamaları, Bazı Temel Şifreleme Yöntemleri, Matrislerle Şifreleme, Açık şifreleme Örnekleri |
| Opsiyonel Program Bileşenleri | Yok |

## Ders Öğrenim Çıktıları

| | |
|---|---|
| 1 | Şifreleme ve şifreleme analizi ile ilgili modern içeriği anlama, |
| 2 | Şifreleme için metodları kullanma ve analiz etme ve bu metodların uygulanabilirliği ve sınırları hakkında düşünme, |
| 3 | Bazı simetrik anahtarlı şifreleme sistemlerini ve açık anahtarlı şifreleme sistemlerinin bazı örneklerini uygulama |
| 4 | Modern simetrik ve açık anahtarlı şifreleme sistemlerinin felsefesini tasarlama ve detayları hakkında tartışma. |

## Haftalık Konular ve İlgili Ön Hazırlık Çalışmaları

| Hafta | Konular | Ön Hazırlık |
|---|---|---|
| 1 | Şifrelemeye Giriş, Tarihçe-Güdüleme. | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 2 | Sayılar Teorisinde Bazı Temel Kavramlar | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 3 | Cebir Adımlarında Zaman Hesaplaması | Kaynaklardaki ilgili bölüm |
| 4 | Bölünebilme ve Öklit Algoritması | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |

| | | |
|---|---|---|
| 5 | Kongrüanslar | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 6 | Çarpanlara Ayırmanın Uygulamaları | Kaynaklardaki ilgili bölüm |
| 7 | Sonlu Cisimler ve Kuadratik Kalanlar | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 8 | Sonlu Cisimler ve Kuadratik Kalanlar | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 9 | Vize | |
| 10 | Kuadratik Kalanlar | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 11 | Bazı Temel Şifreleme Yöntemleri | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 12 | Matrislerle Şifreleme | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 13 | Açık şifreleme | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 14 | RSA | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |
| 15 | Ayrık Logaritmalar, Knapsack | “A Course in Number Theory and Cryptography” by Neal Koblitz, Springer |

## Değerlendirme Sistemi

| **Etkinlikler** | **Sayı** | **Katkı Payı** |
|---|---|---|
| Devam/Katılım | | |
| Laboratuar | | |
| Uygulama | | |
| Arazi Çalışması | | |
| Derse Özgü Staj | | |
| Küçük Sınavlar/Stüdyo Kritiği | | |
| Ödev | | |
| Sunum/Jüri | | |
| Projeler | 1 | 30 |
| Seminer/Workshop | | |
| Ara Sınavlar | 1 | 30 |
| Final | 1 | 40 |
| **Dönem İçi Çalışmaların Başarı Notuna Katkısı** | | 60 |

| | |
|---|---|
| **Final Sınavının Başarı Notuna Katkısı** | 40 |
| **TOPLAM** | 100 |

## AKTS İşyükü Tablosu

| **Etkinlikler** | **Sayı** | **Süresi (Saat)** | **Toplam İşyükü** |
|---|---|---|---|
| Ders Saati | 14 | 3 | 42 |
| Laboratuar | | | |
| Uygulama | | | |
| Arazi Çalışması | | | |
| Sınıf Dışı Ders Çalışması | 14 | 6 | 84 |
| Derse Özgü Staj | | | |
| Ödev | 6 | 5 | 30 |
| Küçük Sınavlar/Stüdyo Kritiği | | | |
| Projeler | 1 | 20 | 20 |
| Sunum / Seminer | | | |
| Ara Sınavlar (Sınav Süresi + Sınav Hazırlık Süresi) | 1 | 2 | 2 |
| Final (Sınav Süresi + Sınav Hazırlık Süresi) | 1 | 2 | 2 |
| | | **Toplam İşyükü** | 180 |
| | | **Toplam İşyükü / 30(s)** | 6.00 |
| | | **AKTS Kredisi** | 6 |

| | |
|---|---|
| Diğer Notlar | Yok |