

0205704 KRİPTOLOJİYE GİRİŞ

Normal Öğretim:

İkinci Öğretim:

Güz 2018-2019

**Dersin Verilme Şekli:** Yüz yüze anlatım

**ÖĞRETİM ELEMANI BİLGİLERİ**

**Dersi Veren Öğretim Elemanı:**

**Ünvanı:**

**Oda no:**

**Tel:**

**Ofis Saati:**

**E-Posta:**

**DESR TANIMI**

**Dersin Kredisi:** *3 (3+0)*

**AKTS**: *5*

**Ders Türü:** *Seçmeli*

**Katalog Tanımı:** *Bu ders modern kriptografi ve iletişim güvenliğine bir giriş sağlar. Kriptografik algoritmaların ve protokollerin nasıl çalıştığı ve nasıl kullanılacağı üzerine odaklanır. Ders, açık anahtar şifreleme, mesaj doğrulama kodları, dijital imzalar ve anahtar oluşturma ve bunun yanı sıra AES, RSA gibi yaygın örnekleri ve kullanımlarını içermektedir.*

**Ön Koşul:** *Yok*

**Ders Kitabı/Önerilen Kaynaklar:**

*Paar, Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners. 1st edition, Springer, 2009.*

*Nigel Smart, Cryptography: An Introduction, Mcgraw-Hill College, 2004.*

*Menezes, van Oorschot, Vanstone: Handbook of Applied Cryptography. CRC Press. 5th printing 2001.*

*J. A. Buchmann, Introduction to Cryptography, Springer-Verlag, New York, 2000.*

*D. R. Stinson, Cryptography: Theory and Practice, CRC, 1995.*

**Dersin Amacı**

|  |  |
| --- | --- |
| *1* | *Bilgisayar güvenliği ve kriptolojinin temel kavramlarını öğretmek* |
| *2* | *Kriptografik yöntemleri tanıtmak* |
| *3* | *Öğrencilere geliştirecekleri uygulamalarda mevcut kriptoloji metotlarını kullanarak veri güvenliğini sağlamalarını öğretmek* |
| *4* | *Öğrencilerin, bilgisayar sistemlerinin güvenliğini anlamalarını ve çözümleyebilmelerini sağlamak* |
| *5* | *Yasal konuları tartışmak* |

**Haftalık Ders Konuları**

|  |  |
| --- | --- |
| *No* |  |
| *1* | *Kriptolojiye Giriş Ve Tarihçesi* |
| *2* | *Kriptolojinin Temelleri* |
| *3* | *Klasik Şifreleme Sistemleri ve Sayılar Teorisi* |
| *4* | *Simetrik Kriptoloji Sistemleri* |
| *5* | *Asimetrik Kriptoloji Sistemleri* |
| *6* | *Veri Şifreleme Standardı (DES)* |
| *7* | *İleri Şifreleme Standardı (AES)* |
| *8* | *Ara Sınavı* |
| *9* | *Anahtar Yönetimi ve Açık Anahtarlar* |
| *10* | *RSA Algoritması* |
| *11* | *Sayısal İmza* |
| *12* | *Hashing Algoritması ve Mesaj Doğrulama* |
| *13* | *Kriptografik Protokoller* |
| *14* | *Yasal Konular* |

**Dersin Öğrenme Çıktıları**

*Bu dersi başarıyla tamamlayan öğrenciler;*

* *Kriptolojinin genel prensiplerini ve genel kriptanalizi anlar*
* *Simetrik şifreleme ve kimlik doğrulama kavramlarını tanır*
* *Açık anahtar şifreleme, dijital imzalar ve anahtar oluşturmayı açıklar*
* *Basit şifreleme çözümlerini oluşturur ve analiz eder*
* *Kriptolojik sistemlerin zayıf yönlerini tespit eder*
* *Güvenliğe ilişkin yasal ve toplumsal konularla ilgili tartışır*

**Değerlendirme Yöntemleri**

|  |  |
| --- | --- |
| *1. Ara Sınav* | *40%* |
| *2. Final Sınavı* | *60%* |

***Dersin Mesleki Bileşene Katkısı***

|  |  |
| --- | --- |
| *Temel Mühendislik* | *40%* |
| *İnsan ve Toplum Bilimi* | *0%* |
| *Matematik ve Temel Bilimler* | *60%* |

**Ders Tanıtımını Hazırlayan Kişi/Hazırlanma Tarihi**

*Şeyma Cihan, Haziran 2018*

**Son Revizyon Tarihi**

*Haziran 2018*