# İTÜ
# LİSANSÜSTÜ DERS KATALOG FORMU
## (GRADUATE COURSE CATALOGUE FORM)

| **Dersin Adı** | **Course Name** |
|---|---|
| Saldırı Saptama ve Önleme | Intrusion Detection and Prevention |

| **Kodu (Code)** | **Yarıyılı (Semester)** | **Kredisi (Local Credits)** | **AKTS Kredisi (ECTS Credits)** | **Ders Seviyesi (Course Level)** |
|---|---|---|---|---|
| BGK 506 | Güz/Bahar (Fall/Spring) | 3 | 7,5 | Y.L. (M.Sc.) |

| | | | |
|---|---|---|---|
| **Lisansüstü Program (Graduate Program)** | Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography) | | |
| **Dersin Türü (Course Type)** | Zorunlu ( Compulsory ) | **Dersin Dili (Course Language)** | Türkçe/İngilice (Turkish/English) |

| | |
|---|---|
| **Dersin İçeriği**<br><br>**(Course Description)**<br><br>*30-60 kelime arası* | Bilgi sistemlerine yönelik saldırı türleri, Saldırılara karşı geliştirilen yöntemler ve teknikler: Saldırı türüne özel karşı önlemler, Sezgisel önlemler, Bilgi sistemini izleme yöntemleri, Kötü niyetli davranışların saptanması, Güvenlik açıklarının incelenmesi, Önleme yöntemlerinin geliştirilmesi |
| | Varieties of attacks to information systems. Counter measures and techniques. Counter measures against a specific type of attack. Heuristic methods. Monitoring methods. Determining malicious logic. Analysis of security flaws. Enhancing protective methods. |
| **Dersin Amacı**<br><br>**(Course Objectives)**<br><br>*Maddeler halinde 2-5 adet* | • Saldırı saptama yöntemlerinin tartışılması<br>• Yaygın saldırılara karşı kullanılabilecek önlemlerin tanıtılması<br>• Tanıtılan önlemlerin uygulanması |
| | • Discussing intrusion detection mechanisms<br>• Introducing counter measures against common types of attacks<br>• Application of introduced mechanisms |
| **Dersin Öğrenme Çıktıları**<br><br>**(Course Learning Outcomes)**<br><br>*Maddeler halinde 4-9 adet* | Öğrenciler<br>1. İyi bilinen saldırıları tanıyacaklardır.<br>2. İyi bilinen saldırılara karşı uygulanan iyi savunma reçeteleri edineceklerdir.<br>3. Bir deney ortamı içinde saldırıyı saptama konusunda deneyim kazanacaklardır.<br>4. Bir deney ortamı içinde bir saldırıyı engelleme konusunda deneyim kazanacaklardır. |
| | 1. Common types of attacks<br>2. Best practices against common types of attacks<br>3. Intrusion detection in an environmental setup<br>4. Intrusion prevention in an environmental setup |

| | |
|---|---|
| **Kaynaklar**<br><br>**(References)**<br><br>*En önemli 5 adedini belirtiniz* | 1. The State of the Art in Intrusion Prevention and Detection, Al-Sakib Khan Pathan, 2014, Auerbach Publications.<br>2. Network Security Assessment: Know Your Network, 2nd Ed., Chris McNab, 2007, O'Reilly Media.<br>3. Security Strategies In Web Applications And Social Networking, Mike Harwood, Marcus Goncalves, Matthew Pemble, 2010, Jones & Bartlett Learning.<br>4. IT Audit, Control, and Security, 2nd Ed., Robert R. Moeller, 2010, Wiley.<br>5. Information Assurance Architecture, Keith D. Willett, 2008, Auerbach Publications. |
| **Ödevler ve Projeler**<br><br>**(Homework & Projects)** | 1 Dönem Ödevi<br>1 Term Paper |
| **Laboratuar Uygulamaları**<br><br>**(Laboratory Work)** | --<br>-- |
| **Bilgisayar Kullanımı**<br><br>**(Computer Use)** | --<br>-- |
| **Diğer Uygulamalar**<br><br>**(Other Activities)** | --<br>-- |

**Başarı Değerlendirme Sistemi**

**(Assessment Criteria)**

| **Faaliyetler (Activities)** | **Adedi* (Quantity)** | **Değerlendirmedeki Katkısı, % (Effects on Grading, %)** |
|---|---|---|
| **Yıl İçi Sınavları (Midterm Exams)** | 1 | % 30 (30 %) |
| **Kısa Sınavlar (Quizzes)** | - | - |
| **Ödevler (Homework)** | - | - |
| **Projeler (Projects)** | - | - |
| **Dönem Ödevi/Projesi (Term Paper/Project)** | 1 | % 30 (30%) |
| **Laboratuar Uygulaması (Laboratory Work)** | - | - |
| **Diğer Uygulamalar (Other Activities)** | - | - |
| **Final Sınavı (Final Exam)** | 1 | % 40 (40%) |

*****Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

# DERS PLANI

| Hafta | Konular | Dersin Çıktıları |
|---|---|---|
| **1** | Açık, tehdit ve saldırı kavramları | |
| **2** | Saldırı türleri ve sınıflandırılması | |
| **3** | Saldırı türlerine yönelik iyi bilinen savunma yöntemleri | |
| **4** | Sınıflandırılmış bilgiye dayalı savunma yöntemleri | |
| **5** | Kestirimsel savunma yöntemleri | |
| **6** | Bilgi sistemlerinin izlenmesi | |
| **7** | Kötü niyetli davranışların sezilmesi | |
| **8** | Sistem içi saldırılarda izlenecek yöntemler | |
| **9** | Güncel tehditler | |
| **10** | Seçilen örnek bir tehdide karşı savunma tasarlama (Tartışma ve akıl yürütme) | |
| **11** | Güncel tehditler | |
| **12** | Seçilen örnek bir tehdide karşı savunma tasarlama (Tartışma ve akıl yürütme) | |
| **13** | Güncel yayınlar | |
| **14** | Güncel yayınlar | |

# COURSE PLAN

| Weeks | Topics | Course Outcomes |
|---|---|---|
| **1** | Vulnerability, threat and attack | |
| **2** | Attack types and their classification | |
| **3** | Common defense methods against common attacks | |
| **4** | Defense methods based on classified data | |
| **5** | Defense methods based on heuristics | |
| **6** | Monitoring information systems | |
| **7** | Detecting malicious behavior | |
| **8** | Defense methods against insider attacks | |
| **9** | Up-to-date threats | |
| **10** | Design a defense approach based on a selected threat (Discussion and induction) | |
| **11** | Up-to-date threats | |
| **12** | Design a defense approach based on a selected threat (Discussion and induction) | |
| **13** | Paper discussion | |
| **14** | Paper discussion | |

## Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programıyla İlişkisi

| | Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar) | Katkı Seviyesi | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| **i.** | Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği Mühendisliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi). | | X | |
| **ii.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi). | X | | |
| **iii.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri). | | X | |
| **iv.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri). | X | | |
| **v.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri). | | X | |
| **vi.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği). | | | |
| **vii.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği). | | | |
| **viii.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği). | | | |
| **ix.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği). | | X | |
| **x.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik). | X | | |
| **xi.** | Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik). | X | | |
| **xii.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik). | | | X |
| **xiii.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik). | | X | |
| **xiv.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik). | X | | |
| **xv.** | Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik). | X | | |
| **xvi.** | Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik). | X | | |

**1: Az, 2. Kısmi, 3. Tam**

**Relationship between the Course and Cybersecurity Engineering and Cryptography Graduate (MS) Curriculum**

| | Program Outcomes | Level of Contribution | | |
|---|---|---|---|---|
| | | 1 | 2 | 3 |
| **i.** | Developing and intensifying knowledge in Cybersecurity Engineering and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge). | | X | |
| **ii.** | Grasping the inter-disciplinary interaction related to Cybersecurity Engineering and Cryptography area (knowledge). | X | | |
| **iii.** | The ability to use the expert-level theoretical and practical knowledge acquired in Cybersecurity Engineering and Cryptography area (skill). | | X | |
| **iv.** | Interpreting and forming new types of knowledge by combining the knowledge from Cybersecurity Engineering and Cryptography area and the knowledge from various other disciplines (skill). | X | | |
| **v.** | Solving the problems faced in Cybersecurity Engineering and Cryptography area by making use of the research methods (skill). | | X | |
| **vi.** | The ability to carry out a specialist study related to Cybersecurity Engineering and Cryptography area independently (Competence to work independently and take responsibility). | | | |
| **vii.** | Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Cybersecurity Engineering and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility). | | | |
| **viii.** | Fulfilling the leader role in the environments where solutions are sought for the problems related to Cybersecurity Engineering and Cryptography area (Competence to work independently and take responsibility) | | | |
| **ix.** | Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence). | | X | |
| **x.** | Systematically transferring the current developments in Cybersecurity Engineering and Cryptography area and one's own work to other groups in and out of Cybersecurity Engineering and Cryptography area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency). | X | | |
| **xi.** | Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency). | X | | |
| **xii.** | Using the computer software together with the information and communication technologies efficiently and according to the needs of Cybersecurity Engineering and Cryptography area (Communication and Social Competency). | | | X |
| **xiii.** | Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Cybersecurity Engineering and Cryptography area related data and the ability to teach these values to others (Area Specific Competency). | | X | |
| **xiv.** | Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency). | X | | |
| **xv.** | Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency). | X | | |
| **xvi.** | The ability to present one's own work within the international Cybersecurity Engineering and Cryptography environments orally, visually and in written forms (Area Specific Competency). | X | | |

**1: Little, 2. Partial, 3. Full**

| ***Düzenleyen (Prepared by)*** | ***Tarih (Date)*** | ***İmza (Signature)*** |
|---|---|---|
| Prof. Dr. Eşref ADALI | 31.03.2014 | |