

İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

| | | | | | |
|--|---|------------------------------------|--|---|--|
| Dersin Adı | | | | Course Name | |
| Bulut Bilişim Güvenliği | | | | Security for Cloud Computing | |
| Kodu (Code) | Yarıyılı (Semester) | Kredisi (Local Credits) | AKTS Kredisi (ECTS Credits) | Ders Seviyesi (Course Level) | |
| BGK 512E | 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) | Seçmeli (Elective) | | Dersin Dili (Course Language) | İngilizce/Türkçe (English/Turkish) | |
| Dersin İçeriği (Course Description) | Bulut bilişim altyapısı, kuralları. Bulut bilişime özgü güvenlik sorunları, Özel, kamu, kurum ve karma bulutlar için mimari ve altyapılar, Sanallaştırma güvenliği, Uygulama güvenliği, Bulutlarda politika ve risk değerlendirmesi, Bulut ortamlarında sözleşme hükümleri, Grid servisleri ve uzaktan güvenlik denetimleri, SaaS, PaaS ve IaaS kavramları ve güvenlik modelleri | | | | |
| <u>30-60 kelime arası</u> | Cloud computing infrastructure. Cloud computing rules. Security problems specific to cloud computing. Architecture and infrastructures for private, public, institutional and hybrid clouds. Virtualization security. Application security. Policy and risk assessment for clouds. Contracts and agreements in clouds. Grid services and remote security control. SaaS, PaaS, IaaS concepts. Security models. | | | | |
| Dersin Amacı (Course Objectives) | <ul style="list-style-type: none">Bulut bilişim konusunda öğrencilerin ufkunu açmakBulut yapısını, var olan sistemlerden farklarını ve benzerliklerini ortaya koymakBulut bilişimin getirdiği güvenlik açıkları üzerine akıl yürütmek ve önlemler önermek | | | | |
| <u>Maddeler halinde 2-5 adet</u> | <ul style="list-style-type: none">Teaching cloud computing conceptComparing cloud with existing structuresDiscussing and proposing solutions to the cloud specific security problems | | | | |
| Dersin Öğrenme Çıktıları (Course Learning Outcomes) | Öğrenciler | | | | |
| <u>Maddeler halinde 4-9 adet</u> | <ol style="list-style-type: none">Bulut bilişim kavramını öğrenmişBulut kaynaklı güvenlik sorunlarını tanımışBulutla ilgili güvenlik sorunlarına karşı savunma önerebilecek durumdaBulutla ilgili sorumlulukları tanıyor ve yasal mevzuat konusunda tartışabiliyor Olacaklardır. | | | | |
| | <ol style="list-style-type: none">Cloud computing will be learntCloud specific security problems will be introducedBeing able to propose solutions to cloud security problemsKnowing liabilities and being able to discuss cloud-specific legislation | | | | |

| | | | |
|--|---|------------------------------------|---|
| Kaynaklar (References) <u>En önemli 5 adedini belirtiniz</u> | <ol style="list-style-type: none"> 1. Cloud Computing: Concepts, Technology & Architecture, Thomas Erl, Ricardo Puttini, Zaigham Mahmood, 2013, Prentice Hall. 2. Security and Cryptography: A Guide to Building Dependable Distributed Systems, 2nd Ed., Ross J. Anderson, 2008, Wiley. 3. Writing Secure Code: Practical Strategies and Proven Techniques for Building Secure Applications in a Networked World, 2nd Ed., Michael Howard, David LeBlanc, 2004, Microsoft Press. 4. Managing Risk In Information Systems, Darril Gibson, 2010, Jones & Bartlett Learning. 5. Legal Issues In Information Security, Joanna Lyn Grama, 2010, Jones & Bartlett Learning. | | |
| Ödevler ve Projeler | 1 Dönem Ödevi | | |
| (Homework & Projects) | 1 Term Paper | | |
| Laboratuvar Uygulamaları | -- | | |
| (Laboratory Work) | -- | | |
| Bilgisayar Kullanımı | -- | | |
| (Computer Use) | -- | | |
| Diğer Uygulamalar | -- | | |
| (Other Activities) | -- | | |
| 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%) |
| | Laboratuvar 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 | Bulut kavramı | |
| 2 | Bulut tanımları ve güncel uygulamalar | |
| 3 | Bulutun var olan dizgelerle kıyası | |
| 4 | Bulutta güvenlik sorunları: tarihsel sorunlar | |
| 5 | Bulutta güvenlik sorunları: güncel sorunlar | |
| 6 | Yerleşimden ve kurulumdan kaynaklanabilecek diğer sorunlar | |
| 7 | Bulutta sanallaştırma yöntemleri | |
| 8 | Bulut için genel geçer güvenlik önlemleri | |
| 9 | Mevzuata ilişkin sorunlar | |
| 10 | Güven ilişkilerine dayalı sorunlar | |
| 11 | Güvenli bilgi saklama yöntemleri | |
| 12 | Güvenli bilgi işleme yöntemleri | |
| 13 | Güvenli asıllama yöntemleri ve mahremiyet | |
| 14 | Bulutta saklanan bilgilerin izlenebilirliği | |

COURSE PLAN

| Weeks | Topics | Course Outcomes |
|-------|---|-----------------|
| 1 | Cloud computing concept | |
| 2 | Cloud definitions and up-to-date applications | |
| 3 | Comparison of cloud with existing systems | |
| 4 | Security problems in cloud: inherited historical problems | |
| 5 | Security problems in cloud: cloud-specific problems | |
| 6 | Other problems caused by deployment and installation | |
| 7 | Virtualization methods in cloud | |
| 8 | Common security measures in cloud | |
| 9 | Problems due to legislation | |
| 10 | Problems due to trust relations | |
| 11 | Secure data storage methods | |
| 12 | Secure data processing methods | |
| 13 | Secure authentication and privacy | |
| 14 | Auditability of data in the cloud | |

Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programıyla İlişkisi

| | Programın mezuna kazandıracığı 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 çözümlenebilir (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 özümledikleri 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

| <u>Düzenleyen (Prepared by)</u> | <u>Tarih (Date)</u> | <u>İmza (Signature)</u> |
|---------------------------------|---------------------|-------------------------|
| Prof. Dr. Eşref ADALI | 31.03.2014 | |