İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Şifreleme ve Sayılar Teorisi	Cryptography and Number Theory

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 609E	Güz/Bahar (Fall/Spring)	3	7,5	Doktora (P.Hd.)

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

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	Tarihsel şifreleme tekniklerine başlangıç ve şifreleme analizleri. Açık Anahtarlı Şifreleme (RSA, ElGamal sistemleri). Veri Şifreleme Standardı (DES) ve Gelişmiş şifreleme Standardı (AES). İmza protokolleri ve Anahtar Dağıtımı. Gizli paylaşım politikaları ve hash fonksiyonları. Sıfır Bilgi İspatı. Oval Kavis Aritmetiği. Tam sayı ve modüler aritmetik. Introducing historical techniques of encryption and their cryptanalysis. Public key cryptography (RSA, ElGamal systems). The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). Signature schemes and key distribution. Secret sharing schemes and hash functions. Zero knowledge proofs. Elliptic curves arithmetic. Integer and modular arithmetic.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	1. Şifreleme ve şifre çözme algoritmalarını anlamak ve analiz etmek için yeterli matematiksel alt yapıyı sağlamak. 2. Öğrencileri siber güvenlik alanında zorlu problemlere hazırlamak. 3. Veri depolama, veri paylaşma ve veri transferi konularında güvenli metotlar öğretmek. 1. To provide sufficient mathematical background to understand and analyze encryption/decryption algorithms. 2. To prepare the students for the challenging problems in the area of cybersecurity. 3. To teach secure methods for data storage, data sharing and data transferring.
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Eski ve yeni şifreleme teknikleri hakkında derin bilgi kazanma. 2. Çeşitli türlerde açık ve gizli anahtarlı şifreleme sistemlerini gerçekleştirebilmek. 3. Şifreleme tekniklerinin analizini yapabilmek. 4. Dijital İmza politikalarını öğrenme. 5. Gizli paylaşım politikalarını gerçekleştirebilmek. A Msc/PhD student completing this course successfully should 1. Gain a deep knowledge of old and modern encryption techniques. 2. Be able to implement various types of public-key and private-key cryptosystems. 3. Should be able make cryptanalysis of encryption techniques. 4. Learn digital signature schemes. 5. Be able implement secret sharing schemes.

<table>
<tr><td>Kaynaklar

(References)

En önemli 5 adedini belirtiniz</td><td colspan="3">1) J. KATZ, Y. LINDELL, INTRODUCTION TO MODERN CRYPTOGRAPHY: PRINCIPLES AND PROTOCOLS, CHAPMAN & HALL/CRC, 2007.
2) W. TRAPPE, L. WASHINGTON, INTRODUCTION TO CRYPTOGRAPHY WITH CODING THEORY (2ND EDITION), PEARSON PRENTICE HALL, 2006.
3) R. ANDERSON, SECURİTY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS, WILEY, 2008.
4) A. MENEZES, P. C. VAN OORSCHOT, S. VANSTONE, HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS, 1996.
5) L. WASHINGTON, ELLIPTIC CURVES: NUMBER THEORY AND CRYPTOGRAPHY, 2ND EDITION 2008.</td></tr>
<tr><td rowspan="2">Ödevler ve Projeler

(Homework & Projects)</td><td colspan="3"></td></tr>
<tr><td colspan="3">7 HOMEWORKS AND 2 PROJECTS</td></tr>
<tr><td rowspan="2">Laboratuar Uygulamaları

(Laboratory Work)</td><td colspan="3"></td></tr>
<tr><td colspan="3">7 RECITATION IN COMPUTER LAB</td></tr>
<tr><td rowspan="2">Bilgisayar Kullanımı

(Computer Use) Dersinizde kullnadığınız yazılım ve simulasyon programları yazılabilir</td><td colspan="3">C, C++, MATHEMATICA, PARI, SAGE. MAGMA.</td></tr>
<tr><td colspan="3">C,C++,MATHEMATICA, PARI, SAGE, MAGMA</td></tr>
<tr><td rowspan="2">Diğer Uygulamalar

(Other Activities)</td><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="9">Başarı Değerlendirme Sistemi

(Assessment Criteria)</td><td>Faaliyetler
(Activities)</td><td>Adedi*
(Quantity)</td><td>Değerlendirmedeki Katkısı, %
(Effects on Grading, %)</td></tr>
<tr><td>Yıl İçi Sınavları
(Midterm Exams)</td><td>1</td><td>30%</td></tr>
<tr><td>Kısa Sınavlar
(Quizzes)</td><td></td><td></td></tr>
<tr><td>Ödevler
(Homework)</td><td>7</td><td>20%</td></tr>
<tr><td>Projeler
(Projects)</td><td>2</td><td>10%</td></tr>
<tr><td>Dönem Ödevi/Projesi
(Term Paper/Project)</td><td></td><td></td></tr>
<tr><td>Laboratuar Uygulaması
(Laboratory Work)</td><td></td><td></td></tr>
<tr><td>Diğer Uygulamalar
(Other Activities)</td><td></td><td></td></tr>
<tr><td>Final Sınavı
(Final Exam)</td><td>1</td><td>%40</td></tr>
</table>

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

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Model Şifrelemenin Temel Prensipleri	1
2	Temel Şifreler ve Şifre Analizi	1, 3
3	Gizli Anahtarlı Şifreleme ve **sözde raslantısallık.**	1, 2, 3
4	Açık Anahtarlı Şifreleme (RSA, ElGamal etc)	1, 2, 3
5	**Cryptographic hardness assumptions (RSA problem, factoring integers) !!!**	1, 3
6	Veri şifreleme Standartları ve Gelişmiş şifreleme Standartları	1, 2, 3
7	(Digital) İmza Politikaları	1, 2, 3, 4
8	Rastsal Kahin Modeli içinde Açık Anahtarlı Şifreleme	1, 2, 3
9	Anahtar Dağılımı	1, 2, 3
10	Gizli paylaşım politikaları	1, 3, 5
11	Identity based encryption	1, 2, 3
12	Sıfır Bilgi İspatı	1, 2, 3
13	Oval Kavis	1, 2
14	Tam sayı ve modüler aritmetik.	1, 2

COURSE PLAN

Weeks	Topics	Course Outcomes
1	The fundamental principles of modern cryptography	1
2	Basic Cihpers and their cryptanalysis	1, 3
3	Private-key Encryption and Pseudorandomness	1, 2, 3
4	Public key cryptography (RSA, ElGamal etc)	1, 2, 3
5	Cryptographic hardness assumptions (RSA problem, factoring integers, DLP)	1, 3
6	The Data Encryption Standard and the Advanced Encryption Standard	1, 2, 3
7	Signature schemes	1, 2, 3, 4
8	Public-key cryptosystems in the random oracle model	1, 2, 3
9	Key distribution	1, 2, 3
10	Secret sharing schemes	1, 3, 5
11	Identity based encryption	1, 2, 3
12	Zero-knowledge proofs	1, 2, 3
13	Elliptic curves	1, 2
14	Integer arithmetic and modular arithmetic	1, 2

NOT-1: Ders planı, sadece hafta bazında işlenen ders konularını içermeli, ara ve kısa sınavlar ders planlarına yazılmamalıdır.

Dersin Bilgi Güvenliği Mühendisliği 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 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).			
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).			
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).			
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).			
xv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).			
xvi.	Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).			

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Information Security Engineering 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 Information Security 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 Information Security Engineering area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).			
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).			
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).			
xiv.	Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography ng area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).			
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).			
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).			

1: Little, 2. Partial, 3. Full

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
Y.Doç.Dr. Enver Özdemir	15.05.2014	