İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Kriptografi Mühendisliği	Cryptographic Engineering

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 608E	Güz/Bahar (Fall/Spring)	3	7,5	Dr. (PhD.)

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)** *30-60 kelime arası*	Bu ders kriptografi yazılım ve donanımlarını anlama, modelleme, tasarlama ve sınama Ortak ve yaygın olarak kullanılan teknoloji ve platformlar üzerindeki algoritma, metot ve tekniklerle günümüzdeki en gelişmiş gömülü yazılım ve donanım kriptolarının üretimi.
	Understanding, modeling, designing, developing, testing, and validating cryptographic software and hardware. We study algorithms, methods, and techniques in order to create state-of-art cryptographic embedded software and hardware using common platforms and technologies.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	1. Blok Şifreleme ve Hash(Özet) Algoritmalarının Temellerini Öğrenme 2. Çoklu Keskinli Tamsayı Aritmetiğini Anlama 3. Glois Alanlarını Öğrenme ve Oluşturma 4. Gerçek Deterministtik Rasgele Sayı Üreteci Oluşturma ve Kullanma 5. Yan Kanal Saldırılarını Analiz Etme ve Önleme
	1. To Teach Fundamentals of Block Cipher and Hash Algorithms 2. To Understand Multi-precision Integer Arithmetic 3. To Learn Galois Fields and their Construction 4. Build and Use True and Deterministic Random Number Generators 5. Understand and Apply Side-Channel Analysis and Countermeasures
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Blok Şifreleme ve Hash(Özet) Algoritmalarının Tanım ve Kavramları 2. Çoklu Keskinli Tamsayı Aritmetiğini Anlama ve Kullanma 3. Glois Alanları ve Temelleri 4. DRNG ve TRNG'lerin Önemli Sınıfları 5. TRNG'ler Geliştirme 6. Yan Kanal Analizinin Temel Kavramları 7. Yan Kanal Önleme Algoritmaları
	1. Basic definitions and concepts of block cipher and hash algorithms 2. Understanding and using multi-precision integer arithmetic 3. Galois Fields and their Fundamentals 4. Important classes of DRNGs and TRNGs 5. Evaluating TRNGs 6. Basic concepts of side-channel analysis 7. Side-channel countermeasure algorithms

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*			
Ödevler ve Projeler **(Homework & Projects)**	4 Ödev 4 Homework Assignments		
Laboratuar Uygulamaları **(Laboratory Work)**	2 Laboratuvar ödevi 2 Lab Experiments Assignments		
Bilgisayar Kullanımı **(Computer Use)**	Laboratuvarda gömülü sistemlerle çalışılacaktır Lab Experiments Involve Implementing Cryptography on an Embedded Processors		
Diğer Uygulamalar **(Other Activities)**	-- --		
Başarı Değerlendirme Sistemi **(Assessment Criteria)**	**Faaliyetler (Activities)**	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
	Yıl İçi Sınavları (Midterm Exams)	-	-
	Kısa Sınavlar (Quizzes)	-	-
	Ödevler (Homework)	4	% 60 (60 %)
	Projeler (Projects)	-	-
	Dönem Ödevi/Projesi (Term Paper/Project)	-	-
	Laboratuar Uygulaması (Laboratory Work)	2	% 40 (40 %)
	Diğer Uygulamalar (Other Activities)	-	-
	Final Sınavı (Final Exam)	-	-

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

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Blok Şifreleme, AES ve Hash(Özet) algoritmalarına giriş	
2	Etkili AES yazılımları gerçekleştirme	
3	Gizli anahtar algoritmaları için özel donanımlar	
4	Blok şifreleme modu işlemleri ve tekrar konfigüre edilebilir donanımlar üzerinde gerçekleme	
5	Büyük sayılar aritmetiği	
6	Üslü sayı algoritmaları, ekleme çıkarma zincirleri	
7	Bitişik olmayan formlar ve Montgomery çarpma	
8	Kriptografi için aritmetik metotların yazılım ve donanımsal gerçeklemeleri	
9	Sonlu alanların özellikleri, p ve p^m elementlerinin sonlu alanları	
10	Polinomal, normal ve optimum norm bazları	
11	Toplama, çarpma ve ters çevirme işlemleri için algoritmalar	
12	Fiziksel rastgele sayı üreteçlerinin tasarım ve geliştirme kriterleri	
13	Yan kanal analizinin temelleri	
14	Zamanlama, güç ve elektromanyetik ataklar ve önlemleri	

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Introduction to block ciphers and AES and hash algorithms	
2	Efficient AES software implementations	
3	Specialized hardware for secret key algorithms	
4	Block cipher modes of operation and their implementation on reconfigurable hardware	
5	Arithmetic with large numbers	
6	Exponentiation algorithms and addition and subtraction chains	
7	Non-adjacent forms & Montgomery multiplication	
8	Hardware and software implementation of arithmetic methods for cryptographic applications	
9	Properties of finite fields & Finite fields of p and p^m elements	
10	Polynomial, normal and optimal normal bases	
11	Algorithms for performing addition, multiplication, and inversion operations	
12	Design and evaluation criteria for physical random number generators	
13	Basics of side-channel analysis	
14	Timing, power and electromagnetic attacks, and countermeasures	

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 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).		X	
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).		X	
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).	X		
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).		X	
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).		X	
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)	X		
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).		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 ng 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.Cetin Kaya KOÇ Prof.Dr.Ertuğrul KARAÇUHA	1 Mayis 2014	