İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Kriptografi	**Cryptography**

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 516E	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 (Compulsary)	**Dersin Dili (Course Language)**	İngilizce/Türkçe (English/Turkish)

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	Klasik kriptografi: bazı basit kripto sistemleri, basit kripto sistemlerinin analizi. Shannon teorisi: olasılık teorisi, entropinin özellikleri, çarpım kriptosistemleri. Blok şifreleme algoritmaları: değiştirme-permütasyon ağları, lineer kriptanaliz, farksal kriptanaliz, veri şifreleme standardı (DES), ileri şifrelem standardı (AES), şifreleme modları. Kriptografik özet fonksiyonları: özet fonksiyonları ve veri bütünlüğü, özet fonksiyonlarının güvenliği, iteratif özet fonksiyonları, mesaj doğrulama kodları. RSA kriptosistemi: açık anahtarlı kriptosistemlerine giriş, sayı teorisi. Ayrık logaritma problemine dayalı açık anahtarlı kriptosistemleri: ElGamal kriptosistemi, sonlu cisimler, elliptik eğri kriptosistemi. Sayısal imza: sayısal imza sistemlerinin güvenlik gerekleri, ElGamal sayısal imza sistemi, DSA, ECDSA.
	Classical cryptography: introduction: some simple cryptosystems, cryptanalysis of simple cryptosystems. Shannon's theory: probability theory, entropy, properties of entropy, product cryptosystems. Block ciphers: substiturion-permutation network, linear cryptanalysis, differential cryptanalysis, the data encryption standard (DES), advanced encryption standard (AES), modes of operation. Hash functions: collision-free hash functions, authentication codes. The RSA system and factoring: introduction to public-key cryptography, more number theory, the RSA cryptosystem. Public-key cryptosystems based on discrete logarithm problem: the ElGamal cryptosystem, finite field and elliptic curve systems, galois fields, elliptic curves. Signature schemes: introduction, the ElGamal signature scheme, the digital signature algorithm (DSA), the elliptic curve digital signature algorithm (ECDSA).
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	• Klasik kriptosistemlerini öğretmek. • Shannon teorisini öğretmek. • Blok şifreleme algoritmalarını ve yapılan atakları öğretmek. • Özet fonksiyonlarını öğretmek. • Açık anahtarlı kriptosistemlerini öğretmek. • Sayısal imza algoritmalarını öğretmek.
	• To teach classical cryptography. • To teach Shannon's Theory • To teach block ciphers and attacks • To teach hash functions • To teach public key cryptosystems • To teach digital signature algorithms
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	Bu dersi başarıyla tamamlayan yüksek lisans/doktora öğrencileri aşağıdaki konularda bilgi, beceri ve yetkinlik kazanırlar; 1. Klasik kriptografi sistemlerinin hangi sebeple nasıl geliştiğini öğrenirler. 2. Olasılık teorisini, entropinin özellikleri öğrenir, çarpım kriptosistemlerini inceleyebilirler. 3. Değiştirme-permütasyon ağlarını öğrenirler ve bunlar üzerinde lineer ve farksal kriptanaliz uygulayabilirler. 4. Veri şifreleme standardı (DES) ve ileri şifrelem standardını (AES) gerçekleyebilirler. 5. Kriptografik özet fonksiyonlarını inceleyebilir ve gerçekleyebilirler. 6. RSA kriptosistemini gerçekleyebilirler. 7. ElGamal ve elliptik eğri kriptosistemlerini inceleyip gerçekleyebilirler. 8. ElGamal sayısal imza sistemi, DSA ve ECDSA öğrenirler. bilimlerindeki uygulamalarını öğrenmek.

	M.Sc students who successfully pass this course will gain the knowledge, skill and competency in the following subjects; 1. They learn how the classical cryptosystems were progressed. 2. They learn probability theory, entropy, properties of entropy and can investigate about product cryptosystems 3. They learn substiturion-permutation networks and can apply linear and differential cryptanalysis on them. 4. They can implement the data encryption standard (DES) and advanced encryption standard (AES) 5. They can investigate and implement the hash functions. 6. They can implement the RSA cryptosystem. 7. They can investigate and implement the ElGamal and elliptic curve cryptosystems. 8. They learn the ElGamal signature scheme, the digital signature algorithm (DSA), the elliptic curve digital signature algorithm (ECDSA).

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	[1] Stinson, D. R., 2005. Cryptography: Theory and Practice, Chapman and Hall/CRC; 3 edition. [2] Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, Wiley; 2nd edition. [3] Paar, C., 2010. Jan Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners, Springer; 1st Edition.2nd Printing edition. [4] Ferguson, N., Schneier, B., Kohno, T., 2010. Cryptography Engineering: Design Principles and Practical Applications, Wiley; 1 edition.		
Ödevler ve Projeler **(Homework & Projects)**	3 Ödev 2 Homeworks		
Laboratuar Uygulamaları **(Laboratory Work)**	-- --		
Bilgisayar Kullanımı **(Computer Use)**	Ödevler İçin For Homeworks		
Diğer Uygulamalar **(Other Activities)**	-- --		
Başarı Değerlendirme Sistemi **(Assessment Criteria)**	**Faaliyetler (Activities)**	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
	Yıl İçi Sınavları (Midterm Exams)	2	% 60 (60 %)
	Kısa Sınavlar (Quizzes)	-	-
	Ödevler (Homework)	3	%30 (40%)
	Projeler (Projects)	-	-
	Dönem Ödevi/Projesi (Term Paper/Project)		
	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	Klasik kriptografi: bazı basit kripto sistemleri	1
2	Basit kripto sistemlerinin analizi	1
3	Shannon teorisi: olasılık teorisi, entropinin özellikleri	2
4	Çarpım kriptosistemleri	2
5	Blok şifreleme algoritmaları: değiştirme-permütasyon ağları	3
6	Lineer kriptanaliz	3
7	Farksal kriptanaliz	3
8	Veri şifreleme standardı (DES), ileri şifrelem standardı (AES)	4
9	Şifreleme modları	4
10	Kriptografik özet fonksiyonları: özet fonksiyonları ve veri bütünlüğü, özet fonksiyonlarının güvenliği	5
11	İteratif özet fonksiyonları, mesaj doğrulama kodları	5
12	RSA kriptosistemi: açık anahtarlı kriptosistemlerine giriş, sayı teorisi	6
13	Ayrık logaritma problemine dayalı açık anahtarlı kriptosistemleri: ElGamal kriptosistemi, sonlu cisimler, elliptik eğri kriptosistemi	7
14	Sayısal imza: sayısal imza sistemlerinin güvenlik gerekleri, ElGamal sayısal imza sistemi, DSA, ECDSA.	8

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Classical cryptography: introduction: some simple cryptosystems	1
2	Cryptanalysis of simple cryptosystems	1
3	Shannon's theory: probability theory, entropy, properties of entropy	2
4	Product cryptosystems	2
5	Block ciphers: substiturion-permutation network	3
6	Linear cryptanalysis	3
7	Differential cryptanalysis	3
8	The data encryption standard (DES), advanced encryption standard (AES)	4
9	Modes of operation	4
10	Hash functions: collision-free hash functions	5
11	Authentication codes	5
12	The RSA system and factoring: introduction to public-key cryptography, more number theory	6
13	Public-key cryptosystems based on discrete logarithm problem: the ElGamal cryptosystem, finite field and elliptic curve systems, galois fields, elliptic curves	7
14	Signature schemes: introduction, the ElGamal signature scheme, the digital signature algorithm (DSA), the elliptic curve digital signature algorithm (ECDSA)	8

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, Bilişim Uygulamaları alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).			X
ii.	Bilişim Uygulamaları alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).		X	
iii.	Bilişim Uygulamaları alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).			X
iv.	Bilişim Uygulamaları alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).	X		
v.	Bilişim Uygulamaları alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri).			X
vi.	Bilişim Uygulamaları alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).		X	
vii.	Bilişim Uygulamaları 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.	Bilişim Uygulamaları alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Bilişim Uygulamaları alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).			
x.	Bilişim Uygulamaları 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).			
xii.	Bilişim Uygulamaları alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			X
xiii.	Bilişim Uygulamaları 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.	Bilişim Uygulamaları alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			
xv.	Bilişim Uygulamaları alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).			
xvi.	Kendi çalışmalarını, Bilişim Uygulamaları alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).			

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 Informatics Applications area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).			X
ii.	Grasping the inter-disciplinary interaction related to Informatics Applications area (knowledge).		X	
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Informatics Applications area (skill).			X
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Informatics Applications area and the knowledge from various other disciplines (skill).	X		
v.	Solving the problems faced in Informatics Applications area by making use of the research methods (skill).			X
vi.	The ability to carry out a specialist study related to Informatics Applications 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 Informatics Applications 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 Informatics Applications 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.	Systematically transferring the current developments in Informatics Applications area and one's own work to other groups in and out of Informatics Applications 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).			
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Informatics Applications area (Communication and Social Competency).			X
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Informatics Applications 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 Informatics			

	Applications 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 Informatics Applications environments orally, visually and in written forms (Area Specific Competency).			

1: Little, 2. Partial, 3. Full

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