İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Ayrık Matematik	**Discrete Mathematics**

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 505E	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*	Sıra kavramı ve bilgisayar bilimlerinde sıranın önemi. Noether sırası, tüme varımda kullanımı. Özyinelemeli fonksiyonlara uygulanması. Modül bağıntısı, modüler aritmetik ve ilgili teoremler. Çinli kalanlar teoremi ve uygulamaları. Sayma teknikleri ve tekrarlı kombinezonlar. Grup kuramı, kongrüans, yapı benzerlikleri. Permütasyon fonksiyonları ve Polya teoremi. Grup kodları, hata sezme düzeltmede kullanılmaları.
	Order concept, its importance in computer science. Noether order, induction principles. Application to recursive functions. Modulo relation, modular arithmetic and its theorems. Chinese remainder theorem and applications. Counting and multiple combinations. Group theory, congruence relation, homomorphism. Permutation functions and Polya theorem. Group codes, their utilization in fault detection and correction.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	Bu derste işlenen matematik konuları bilgisayar mühendisliğine ilişkin araştırma ve uygulamalarda gerekli matematik bilgilerini tamamlamaktadır. Özellikle kriptoloji ve veri iletme ve saklamada hata sezme ve düzeltme tekniklerinde kullanılan matematiğin altyapısı bu derste verilmektedir.
	The mathematical subjects given in this course are necessary to understand several research areas and applications in computer engineering. Especially, basic mathematical concepts used in cryptology and also in error detection and correction techniques for storage and transmissions are given in this course.
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Tüme varım tekniklerini öğrenmek. 2. Modüler aritmetiği öğrenmek 3. Karmaşık sayma tekniklerini gözden geçirmek. 4. Permütasyon fonksiyonlarını ve Polya teoremini öğrenmek. 5. Grup kuramını ve bilgisayar bilimlerindeki uygulamalarını öğrenmek.
	1. To learn induction techniques 2. To study modular arithmetic theorems. 3. To study complex counting methods. 4. To learn permutation functions and Polya teorem. 5. To study group theory and its application in computer science

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	[1] Grimaldi, R. P., 2004.Discrete and Combinatorial Mathematics: An Applied Introduction, 5/E . [2] Liu, C. L., 1987. Elements of Discrete Mathematics, McGraw Hill. [3] Rosen, K. H., 2003. Discrete Mathematics and Its Applications, McGraw Hill. [4] Jr., M. H. F., 1993. Discrete Mathematics with Applications, John Wiley and Sons. [5] Stanat, D. F., and McAllist, D. F., 1977. Discrete Mathematics in Computer Science, Prentice Hall. [6] Preparata, F. P., and Yeh, R. T., 2004. Introduction to Discrete Structures, Addison Wesley.		
Ödevler ve Projeler **(Homework & Projects)**			
Laboratuar 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)	2	% 60 (60 %)
	Kısa Sınavlar (Quizzes)	-	-
	Ödevler (Homework)	6	%0 (0%)
	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	Tamsayı Sistemleri. Peano aksiyomları	1
2	Noether Sırası. Tüme varım ilkeleri.	1
3	Bölünebilirlik. Asal sayılar.	2
4	Göreli asallık. "mod" kongrüans bağıntısı.	2
5	Fermat ve Euler teoremleri	2
6	Çinli kalanlar teoremi	2
7	Sayma teknikleri ve çoklu kombinezonlar .	3
8	Cebirsel yapılar ve gruplar.	4-5
9	Kongrüans ve yapı benzerlikleri.	4-5
10	Permütasyonlar. Çevrimli gruplar	4
11	Burnside teoremi. Polya döküm çıkarma teoremi	4
12	Eşkümeler ve bölüm yapılar.	5
13	Grup kodları	5
14	Hata sezme ve düzeltme	5

COURSE PLAN

Weeks	Topics	Course Outcomes
1	System of Integers: Peano postulates.	1
2	Noether order. Induction principles.	1
3	Divisibility. Primes.	2
4	Relative primality. "mod" congruence relation.	2
5	Fermat and Euler theorems.	2
6	Chinese remainder theorems.	2
7	Counting and multiple combinations	3
8	Algebraic structures: groups.	4-5
9	Congruence and Homomorphism.	4-5
10	Permutations. Cyclic Groups .	4
11	Burnside Theorem. Polya's method of enumeration	4
12	Cosets and Quotient Structures	5
13	Group Codes	5
14	Error Detection and Correction	5

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).			
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	
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).			
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).			
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).			X
xvi.	Kendi çalışmalarını, Bilişim Uygulamaları 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 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).			
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	
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).			
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).			
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).			X
xvi.	The ability to present one's own work within the international Informatics Applications 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	