İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Kriptolojideki Sayılar Teorisi Problemleri	Computational Number Theory Problems in Cryptography

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
HBM5XXE	Guz (Fall)	3	7.5	YL (M.Sc.)

Lisansüstü Program (Graduate Program)	Hesaplamalı Bilim ve Mühendislik Yüksek Lisans Programı (Computational Science and Engineering Masters Programme)		
Dersin Türü (Course Type)	Seçmeli (Elective)	**Dersin Dili (Course Language)**	İngilizce English

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	Sayılar teorisindeki kriptoloji ile alakalı problemler, sayılar teorisinde yeni araştırma sonuçları, Sayılar teorisinde kavramlar (polinom aritmetiği, eliptik eğri grupları ve eliptik eğri gruplarında grup işlemleri), Latisler ve 2 mertebeli formlar), Çarpanlara ayırma ve asal belirleme algoritmaları
	Theoretical problems related to current cryptosystems, recent research and developments on the subject, number theoretical tools (polynomial arithmetic, elliptic curve groups, arithmetic in elliptic curve groups, lattices and quadratic forms), algorithms used in practice for primality test and integer factorizations
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	1. Sayılar teorisindeki kriptoloji ile alakalı problemlerin öğretilmesi. 2. Sayılar teorisindeki aygıtların, iki mertebeli formlar, eliptik eğriler vb. tanıtılması. 3. Tam sayılar/modüler/eliptik eğrilerinin aritmetiğinde kullanılan algoritmaların ve çarpanlara ayırma algoritmalarının öğretilmesi.
	1. Teach number theoretical problems, which are related to crypto systems. 2. Introduce number theoretical tools such as quadratic forms, elliptic curves. 3. Teach the algorithms used in practice for integer/modular/elliptic curve arithmetic and integer factorization.
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.** Sayılar teorisindeki kriptoloji ve kodlama teorisi sorularını öğrenmiş olur. **2.** Latislerdeki ve 2 mertebeli formlardaki grup işlemlerini yapabilmeli. **3.** Eliptik eğrilerini ve eliptik eğri gruplarındaki grup işlemlerini öğrenmiş olmalı. **4.** Çarpanlara ayırma, asal belirleme ve kok bulma vb. için kullanılan algoritmaları kullanabilmeli. **5.** Bilgisayar ortamında soruları çözmede kendini geliştirmiş olmalı.
	M.Sc./Ph.D. students who successfully pass this course gain knowledge, skill and competency in the following subjects; **1.** Learn the main problems in number theory related to cryptography and coding theory. **2.** Be able to perform operations in lattices and quadratic forms, **3.** Comprehend elliptic curves and arithmetic in elliptic curve groups. **4.** Be able to implement main algorithms for integer factorization, primality test, square roots etc. **5.** Gain skills to solve problems in computer environment.

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	1) R. Crandall, C. Pomerance, Prime Numbers: A Computational Perspective, 2nd Edition, Springer, 2005. 2) H. Cohen, A Course in Computational Algebraic Number Theory, Springer, 2000. 3) L. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd Edition, 2008. 4) H. Cohen, G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press, 2005. 5) D. Cox, Primes of the Form x2+ny2: Fermat, Class Fıeld Theory, and Complex Multıplıcatıon, Wiley, 2013.		
Ödevler ve Projeler **(Homework & Projects)**			
	7 HOMEWORKS AND 2 PROJECTS		
Laboratuar Uygulamaları **(Laboratory Work)**			
Bilgisayar Kullanımı **(Computer Use)** *Dersinizde kullnadığınız yazılım ve simulasyon programları yazılabilir*	**C, C++, PARI, SAGE. MAGMA.**		
	C,C++,PARI, SAGE, MAGMA		
Diğer Uygulamalar **(Other Activities)**			
Başarı Değerlendirme Sistemi **(Assessment Criteria)**	**Faaliyetler (Activities)**	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
	Yıl İçi Sınavları (Midterm Exams)	**1**	**20%**
	Kısa Sınavlar (Quizzes)		
	Ödevler (Homework)	**7**	**30%**
	Projeler (Projects)	**2**	**10%**
	Dönem Ödevi/Projesi (Term Paper/Project)		
	Laboratuar Uygulaması (Laboratory Work)		
	Diğer Uygulamalar (Other Activities)		
	Final Sınavı (Final Exam)	**1**	**%40**

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

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Sayılar Teorisinde Problemler (İkiz Asal, Golbach conjecture, Fermat Sayıları, The Riemann zeta Fonksiyonu, Dirichlet L- Fonksiyonu)	1
2	Sayılar teorisi aygıtları (Modüler Aritmetik, polinom aritmetiği, kare keşfi)	1
3	Eliptik eğrileri, eliptik eğri gruplarında hesaplama	1, 3, 5
4	Polinomlari çarpanlarına ayırma, karekök bulma ve Polinom koku bulma.	1, 4, 5
5	Doğrusal cebir algoritmaları (Gaussian Elimination, doğrusal sistemlerin çözümü, determinant hesaplama)	1, 5
6	Kafesler ve 2 mertebeli formlar (Gram-Schmidt ortogonalleştirmesi, Kafes azaltma algoritmaları	1, 2, 5
7	Asal ve asal olmayan sayıları belirleme: Basit bölme yöntemi, sözde asallar.	1, 4, 5
8	Asal sayı belirleme: n-1 ve n+1 yöntemleri, Gauss toplamı.	1, 2, 4, 5
9	Jacobi toplamı ve AKS test	1, 4, 5
10	Üstel çarpanlara ayırma algoritmaları: Pollard p-1 yöntemi, bebek adımı, dev adımı, 2 mertebeli formlar ve çarpanlara ayırma	1, 2, 4, 5
11	2 mertebeli elek yöntemi	1, 2, 4, 5
12	Sayılar alanı elek yöntemi	1, 2, 4, 5
13	Eliptik eğrilerinde işlemler: eliptik eğri asal belirleme yöntemi	1, 3, 4, 5
14	Eliptik eğrileri çarpanlara ayırma yöntemi	1, 3, 4, 5

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Problems in Number Theory: Twin primes, Golbach conjecture, Fermat numbers, The Riemann zeta function, Dirichlet L-function.	1
2	Number-Theoratical Tools: Modular arithmetic, polynomial arithmetic, square detection.	1
3	Elliptic Curves, computing in elliptic curve groups.	1, 3, 5
4	Polynomial factorization, square roots and polynomial roots.	1, 4, 5
5	Linear algebra algorithms: Gaussian Elimination and solving linear systems, computing determinants.	1, 5
6	Lattices and Quadratic Forms, The Gram-Schmidt orthogonalization procedure, lattice reduction algorithms.	1, 2, 5
7	Recognizing primes and composites: Trial division, Sieving, pseudoprimes.	1, 4, 5
8	Primality proving: the n-1 and n+1 tests, Gauss sums test.	1, 2, 4, 5
9	Jacobi sum test and AKS test	1, 4, 5
10	Exponential factoring algorithms: Pollard p-1 method, Baby steps, giant steps, binary quadratic forms and factoring.	1, 2, 4, 5
11	Subexponential factoring algorithms: Quadratic sieve factorization method	1, 2, 4, 5
12	Number field sieve method	1, 2, 4, 5
13	Elliptic Curve Arithmetic: Elliptic curve primality proving	1, 3, 4, 5
14	Elliptic curve method for factorization	1, 3, 4, 5

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

Dersin Hesaplamalı Bilim ve Mühendislik Programıyla İlişkisi

	Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Hesaplamalı Bilim ve Mühendislik Programındaki bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (*bilgi*).			X
ii.	Alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (*bilgi*).			**X**
iii.	Alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme(*beceri*).			
iv.	Alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (*beceri*).			X
v.	Alanını ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (*beceri*).			X
vi.	Alanını ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme *(Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği)*			
vii.	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.	Alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde aktarabilme *(İletişim ve Sosyal Yetkinlik).*		X	
ix.	Bir yabancı dili en az Avrupa Dil Portföyü B2 genel düzeyinde kullanarak sözlü ve yazılı iletişim kurabilmek *(İletişim ve Sosyal Yetkinlik).*	X		
x.	Alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme *(İletişim ve Sosyal Yetkinlik*)			X
xi.	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).*			
xii.	Alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme *(Alana Özgü Yetkinlik).*			
xiii.	Alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinlerarası çalışmalarda kullanabilme *(Alana Özgü Yetkinlik).*			
xiv.	Hesaplamalı Bilim ve Mühendislik Programında**,** kendi çalışmalarını, alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme *(Alana özgü yetkinlik).*			

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Computational Science and Engineering Program

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in the Computational Science and Engineering program's area, based upon the competency in the undergraduate level (sufficient knowledge) (*knowledge*).			X
ii.	Grasping the inter-disciplinary interaction related to one's area (*knowledge*).			**X**
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in the area (skill).			
iv.	Interpreting and forming new types of knowledge by combining the knowledge from the area and the knowledge from various other disciplines (*skill*).			X
v.	Solving the problems faced in the area by making use of the research methods (*skill*).			X
vi.	The ability to carry out a specialistic study related to one's 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 one's area and coming up with solutions while taking responsibility (*Competence to work independently and take responsibility*).			
viii.	Systematically transferring the current developments in the area and one's own work to other groups in and out of the area; in written, oral and visual forms (*Communication and Social Competency*).		X	
ix.	Proficiency in a foreign language –at least European Language Portfolio B2 Level- and establishing written and oral communication with that language (*Communication and Social Competency*).	X		
x.	Using the computer software together with the information and communication technologies efficiently and according to the needs of the area (*Communication and Social Competency*).			X
xi.	Paying regard to social, scientific, cultural and ethical values during the collecting, Interpreting, practicing and announcing processes of the area related data and the ability to teach these values to others (*Area Specific Competency*).			
xii.	Developing strategy, policy and application plans concerning the subjects related to the area and the ability to evaluate the end results of these plans within the frame of quality processes (*Area Specific Competency*).			
xiii.	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*).			
xiv.	In the Computational Science and Engineering program, the ability to present one's own work within the international environments orally, visually and in written forms (*Area Specific Competency*).			

1: Little, 2. Partial, 3. Full

NOT-2: Ders ile ilgisi olmayan çıktıların boş bırakılması gerekmektedir.

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***