



DERS BİLGİ FORMU

FAKÜLTE / ENSTİTÜ ADI	Fen Edebiyat Fakültesi
BÖLÜM / PROGRAM / ANABİLİM DALI ADI	Matematik
DERSİN ADI	Şifrelemeye Giriş
DERSİN KODU	MAT3260
YEREL KREDİSİ	3
AKTS KREDİSİ	5
HAFTALIK DERS SAATİ	3
HAFTALIK UYGULAMA SAATİ	0
HAFTALIK LABORATUVAR SAATİ	0
ÖNKOŞULLAR	Yok
YARIYIL	Güz, Bahar
DERSİN DİLİ	İngilizce, Türkçe
DERSİN SEVİYESİ	Lisans
DERSİN TÜRÜ	Seçmeli @Matematik Lisans Programı Seçmeli @İlköğretim Matematik Eğitimi Lisans Programı
DERSİN KATEGORİSİ	Temel Meslek Dersleri
DERSİN VERİLİŞ ŞEKLİ	Yüz Yüze
DERSİ SUNAN AKADEMİK BİRİM	Matematik Bölümü
DERSİN KOORDİNATÖRÜ	Emre KOLOTOĞLU
ASİSTAN(LAR)	
DERSİN AMACI	Bu dersin amacı, öğrencilere sayılar teorisi bilgilerinin şifreleme bilimindeki uygulamalarını öğretmektir.
DERSİN İÇERİĞİ	Sayılar teorisinde bazı temel kavramlar, kongrüanslar, çarpanlara ayırma uygulamaları; sonlu cisimler, kuadratik kalanlar; bazı temel şifreleme yöntemleri; açık anahtarlı şifreleme, RSA, ayrık logaritma.
DERS KİTABI / MALZEMESİ / ÖNERİLEN KAYNAKLAR	Ders Kitabı: Koblitz, Neal. <i>A Course in Number Theory and Cryptography</i> . Springer Verlag, 1994.
Ders Öğrenim Çıktıları	Bu dersi başarıyla tamamlayan öğrenciler, - Öklid algoritmasını kullanarak bazı aritmetik hesaplar yapabileceklerdir. - Tekrarlı kare alma algoritmasını kullanabileceklerdir. - Bazı özel çarpanlara ayırma metotlarını kullanabileceklerdir. - Kuadratik kalanların kullanımını gerektiren bazı hesaplamaları yapabileceklerdir. - Bazı basit şifreleme sistemleri ve matrislerle şifreleme yöntemleriyle ilgili uygulamalar yapabileceklerdir. - RSA şifreleme sistemi ve ayrık logaritma problemi ile ilgili uygulamalar yapabileceklerdir.

**DEĞERLENDİRME SİSTEMİ**

Etkinlikler	Sayı	Katkı Payı
Devam/Katılım		
Laboratuvar		
Uygulama		
Arazi Çalışması		
Derse Özgü Staj		
Kısa Sınavlar/Stüdyo Kritiği (Zorunlu): İçerik: Sınav haftasına kadar işlenen konuların tümünü kapsayan kapsamlı sorular Format: Yüz yüze. Klasik kısa sınav (30 dakika) Detaylı Değerlendirme Kriterleri: -Derste işlenen konular ile ilgili problemleri çözebilme	4	%20
Ödev		
Sunum/Jüri		
Proje		
Seminer/Workshop		
Ara Sınavlar: İçerik: Sınav haftasına kadar işlenen konuların tümünü kapsayan kapsamlı sorular Format: Yüz yüze. Klasik sınav. (100 dakika) Detaylı Değerlendirme Kriterleri: - Derste işlenen konular ile ilgili problemleri çözebilme	1	%40
Final: İçerik: Dersin tüm içeriğini kapsayan kapsamlı sorular Format: Yüz yüze. Klasik sınav. (100 dakika) Detaylı Değerlendirme Kriterleri: - Derste işlenen konular ile ilgili problemleri çözebilme	1	%40
Dönem İçi Çalışmaların Başarı Notuna Katkısı		%60
Final Sınavının Başarı Notuna Katkısı		%40
TOPLAM		%100

HAFTALIK KONULAR VE İLGİLİ ÖN HAZIRLIK ÇALIŞMALARI

HAFTALAR	KONULAR	Ön Hazırlık
1	Konu Anlatımı: Şifrelemeye giriş	1. Şifreleme Bilimi ile ilgili araştırma yapılması.
2	Konu Anlatımı: Cebir adımlarında zaman hesaplaması	1. Ders kitabından cebir adımlarında zaman hesaplaması konusunun okunması. Kaynak: Ders Kitabı, 1-10.
3	Konu Anlatımı: Bölünebilme ve Öklid algoritması	1. Ders kitabından bölünebilme ve Öklid algoritması konusunun okunması. Kaynak: Ders Kitabı, 12-15.
4	Kısa Sınav 1 (30 dk.): Ders başında Bölüm 1.1 ve 1.2'yi içeren bir kısa sınav	1. Ders kitabından cebir adımlarında zaman hesaplaması, bölünebilme ve Öklid algoritması konularının tekrar edilmesi.



	Konu Anlatımı: Kongrüanslar	Kaynak: Ders kitabı, 1-10; 12-15. 2. Ders kitabından kongrüanslar konusunun okunması. Kaynak: Ders Kitabı, 19-24.
5	Konu Anlatımı: Çarpanlara ayırma uygulamaları	1. Ders kitabından çarpanlara ayırma uygulamaları konusunun okunması. Kaynak: Ders Kitabı, 27-29.
6	Kısa Sınav 2 (30 dk.): Ders başında Bölüm 1.3 ve 1.4'ü içeren bir kısa sınav Konu Anlatımı: Sonlu cisimler	1. Ders kitabından kongrüanslar ve çarpanlara ayırma uygulamaları konularının tekrar edilmesi. Kaynak: Ders Kitabı, 19-24; 27-29. 2. Ders kitabından sonlu cisimler konusunun okunması. Kaynak: Ders Kitabı, 33-35.
7	Konu Anlatımı: Kuadratik kalanlar	1. Ders kitabından kuadratik kalanlar konusunun okunması. Kaynak: Ders Kitabı, 42-50.
8	Ara Sınav	Sınav haftasına kadar işlenen tüm konuların tekrar edilmesi
9	Konu Anlatımı: Bazı basit şifreleme sistemleri	1. Ders kitabından bazı basit şifreleme sistemleri konusunun okunması. Kaynak: Ders Kitabı, 54-61.
10	Konu Anlatımı: Matrislerle şifreleme	1. Ders kitabından matrislerle şifreleme konusunun okunması. Kaynak: Ders Kitabı, 65-76.
11	Kısa Sınav 3 (30 dk.): Ders başında Bölüm 3.1 ve 3.2'yi içeren bir kısa sınav Konu Anlatımı: Açık anahtarlı şifreleme	1. Ders kitabından bazı basit şifreleme sistemleri ve matrislerle şifreleme konularının tekrar edilmesi. Kaynak: Ders Kitabı, 54-61; 65-76. 2. Ders kitabından açık anahtarlı şifreleme konusunun okunması. Kaynak: Ders Kitabı, 83-89.
12	Konu Anlatımı: RSA	1. Ders kitabından RSA konusunun okunması. Kaynak: Ders Kitabı, 92-95.
13	Konu Anlatımı: Ayrık logaritma	1. Ders kitabından ayrık logaritma konusunun okunması. Kaynak: Ders Kitabı, 97-103.
14	Konu Anlatımı: Knapsack	1. Ders kitabından Knapsack konusunun okunması. Kaynak: Ders Kitabı, 111-115.
15	Kısa Sınav 4 (30 dk.): Ders başında Bölüm 4.1, 4.2, 4.3 ve 4.4'ü içeren bir kısa sınav Konu Anlatımı: Tüm konuların tekrarı	1. Ders kitabından açık anahtarlı şifreleme, RSA, ayrık logaritma, Knapsack konularının tekrar edilmesi. Kaynak: Ders Kitabı, 83-89; 92-95; 97-103; 111-115.
16	Final	İşlenen tüm konuların tekrar edilmesi

AKTS İŞYÜKÜ TABLOSU

Etkinlikler	Sayı	Süresi (Saat)	Toplam İşyükü
Ders Saati	14	3	42
Laboratuvar			
Uygulama (sözlü Sınav)			
Arazi Çalışması			
Sınıf Dışı Ders Çalışması	14	4	56
Derse Özgü Staj			
Ödev			
Küçük Sınavlar/Stüdyo Kritiği	4	6	24
Projeler			
Sunum / Seminer			



Ara Sınavlar (Sınav Süresi + Sınav Hazırlık Süresi)	1	15	15
Final (Sınav Süresi + Sınav Hazırlık Süresi)	1	15	15
Toplam İş yükü:			152
Toplam İş yükü / 30(s):			5.07
AKTS Kredisi:			5



COURSE INFORMATION FORM

FACULTY / GRADUATE SCHOOL	Faculty of Arts and Sciences
DEPARTMENT / PROGRAMME	Mathematics
TITLE OF COURSE	Introduction to Cryptography
CODE	MAT3260
LOCAL CREDIT	3
ECTS	5
LECTURE HOUR / WEEK	3
PRACTICAL HOUR / WEEK	0
LABORATORY HOUR / WEEK	0
PREREQUISITE	None
SEMESTER	Fall, Spring
COURSE LANGUAGE	English, Turkish
LEVEL OF COURSE	First Cycle
COURSE TYPE	Elective @ Bachelor Programme in Mathematics Elective @ Bachelor Programme in Elementary Mathematics Education
COURSE CATEGORY	Core Courses
MODE OF DELIVERY	Face-to-Face
OWNER ACADEMIC UNIT	Department of Mathematics
COURSE COORDINATOR	Emre KOLOTOĞLU
ASSISTANT(S)	
COURSE OBJECTIVES	This course aims to help students learn the use of number theory in cryptography.
COURSE CONTENT	Some topics in elementary number theory, congruences, some applications to factoring; finite fields, quadratic residues; some simple cryptosystems; public key cryptography, RSA, discrete logarithm.
RECOMMENDED OR REQUIRED READINGS	Coursebook: Koblitz, Neal. <i>A Course in Number Theory and Cryptography</i> . Springer Verlag, 1994.
Course Learning Outcomes	Upon successful completion of the course, students will be able to 1. Perform some arithmetic calculations by using the Euclidean algorithm. 2. Use the repeated squaring method. 3. Use some special factorization methods. 4. Perform some calculations that require use of quadratic residues. 5. Perform applications about some simple cryptosystems and methods that use enciphering matrices. 6. Perform applications about RSA cryptosystem and discrete logarithm problem.
EVALUATION SYSTEM	



Activities	Number	Percentage of Grade
Attendance/Participation		
Laboratory		
Application		
Field Work		
Special Work Internship		
Quizzes/Studio Critics: Content: Comprehensive questions covering all topics addressed up to the exam week Format: Face-to-face. Written quiz (30 minutes) Detailed Assessment Criteria: -Ability to solve problems related to the topics covered in the course	4	%20
Homework Assignments		
Presentations/Jury		
Project		
Seminar/Workshop		
Midterms: Content: Comprehensive questions covering all topics addressed up to the exam week Format: Face-to-face. Written exam. (100 minutes). Detailed Assessment Criteria: - Ability to solve problems related to the topics covered in the course	1	%40
Final: Content: Comprehensive questions covering the entire content of the course Format: Face-to-face. Written exam. (100 minutes). Detailed Assessment Criteria: - Ability to solve problems related to the topics covered in the course	1	%40
Percentage of In-Term Studies		%60
Percentage of Final Examination		%40
TOTAL		%100

WEEKLY SUBJECTS AND RELATED PREPARATION STUDIES

WEEKS	COURSE OUTLINE	Related Preparation
1	Lecture: Introduction to cryptography	1. Making research about cryptography
2	Lecture: Time estimates for doing arithmetic	1. Reading the subject time estimates for doing arithmetic from the coursebook. Source: Coursebook, 1-10.
3	Lecture: Divisibility and the Euclidean algorithm	1. Reading the subject divisibility and the euclidean algorithm from the Coursebook. Source: Coursebook, 12-15.
4	Quiz 1 (30 minutes): A short quiz from Chapter 1.1 and 1.2 at the beginning of the lecture Lecture: Congruences	1. Reviewing the subjects time estimates for doing arithmetic, divisibility and the euclidean algorithm from the coursebook. Source: Coursebook, 1-10, 12-15. 2. Reading the subject congruences from the coursebook.



		Source: Coursebook,19-24.
5	Lecture: Some applications to factoring	1. Reading the subject some applications to factoring from the coursebook. Source: Coursebook 27-29.
6	Quiz 2 (30 minutes): A short quiz from Chapter 1.3 and 1.4 at the beginning of the lecture Lecture: Finite fields	1. Reviewing the subjects congruences and some applications to factoring from the coursebook. Source: Coursebook, 27-29. 2. Reading the subject finite fields from the coursebook. Source: Coursebook, 33-35.
7	Lecture: Quadratic residues and reciprocity	1. Reading the subject quadratic residues and reciprocity from the coursebook. Source: Coursebook, 42-50.
8	Midterm	Review of all topics covered up to the exam week.
9	Lecture: Some simple cryptosystems	1. Reading the subject some simple cryptosystems from the coursebook. Source: Coursebook, 54-61.
10	Lecture: Enciphering matrices	1. Reading the subject enciphering matrices from the coursebook. Source: Coursebook, 65-76.
11	Quiz 3 (30 minutes): A short quiz from Chapter 3.1 and 3.2 at the beginning of the lecture Lecture: Public key cryptography	1. Reviewing the subjects some simple cryptosystems and enciphering matrices from the coursebook. Source: Coursebook, 54-61; 65-76. 2. Reading the subject public key cryptography from the coursebook. Source: Coursebook, 83-89.
12	Lecture: RSA	1. Reading the subject RSA from the coursebook. Source: Coursebook, 92-95.
13	Lecture: Discrete logarithm	1. Reading the subject discrete logarithm from the coursebook. Source: Coursebook, 97-103.
14	Lecture: Knapsack	1. Reading the subject Knapsack from the coursebook. Source: Coursebook, 111-115.
15	Quiz 4 (30 minutes): A short quiz from Chapter 4.1, 4.2, 4.3, and 4.4 at the beginning of the lecture Lecture: Review	1. Reviewing the subjects public key cryptography, RSA, discrete logarithm and knapsack from the coursebook. Source: Coursebook, 83-89; 92-95; 97-103; 111-115.
16	Final	Review of all topics covered.

ECTS WORKLOAD TABLE

Activities	Number	Duration (Hour)	Total Workload
Course Hours	14	3	42
Laboratory			
Application			
Field Work			
Study Hours Out of Class	14	4	56
Special Course Internship (Work Placement)			
Homework Assignments			
Quizzes/Studio Critics	4	6	24
Project			
Presentations / Seminar			
Mid-Terms (Examination Duration + Examination Prep. Duration)	1	15	15
Final (Examination Duration + Examination Prep. Duration)	1	15	15
Total Workload:			152
Total Workload / 30(h):			5.07
ECTS Credit:			5



Ders Öğrenim Çıktısı & Program Çıktısı Matrisi

	DÖC-1	DÖC-2	DÖC-3	DÖC-4	DÖC-5	DÖC-6
PC-1 Geometri, analiz, lineer cebir, soyut matematik, cebir ve diferansiyel denklemler gibi matematiğin temel alanlarındaki tanımları ve teoremleri ifade edebilecek, bunlar arasında ilişki kurabilecek ve teoremlerin uygulamalarını açıklayabileceklerdir. / State the definitions and theorems in fundamental areas of mathematics such as geometry, analysis, linear algebra, abstract mathematics, and differential equations, establish connections between them and explain their applications.	=	=	=	=	=	=
PC-2 Matematik alanındaki teorik ve uygulamalı bilgilerini ve matematiksel düşünme becerilerini kullanarak standart ve karmaşık matematiksel problemleri tanımlayabilecek ve analitik ve/veya sayısal yöntemlerle çözebilecek ve matematiksel bir önermenin geçerliliğini farklı ispat yöntemleri ile ispatlayabileceklerdir. / Identify standard and complex mathematical problems, solve these problems with analytical and/or numerical methods and prove the validity of a mathematical proposition through various proof techniques using their theoretical and applied knowledge of mathematics and mathematical thinking skills.	4	4	4	4	=	=
PC-3 Matematik alanındaki teorik ve uygulamalı bilgilerini ve matematiksel düşünme becerilerini kullanarak gerçek hayattaki problemlerin matematiksel modellerini geliştirebilecek ve bu modelleri kullanarak problemlere geçerli çözümler üretebileceklerdir. / Develop mathematical models for real-life problems and generate valid solutions based on these models using their theoretical and applied knowledge of mathematics and mathematical thinking skills.	=	=	=	=	4	4
PC-4 Disiplinlerarası bir yaklaşımla, farklı alanlarda edinmiş oldukları bilgileri sentezleyebileceklerdir. / Synthesise knowledge acquired from different disciplines through an interdisciplinary approach.	=	=	=	=	=	=
PC-5 Matematik alanında edindikleri bilgi birikimlerini ve matematiksel düşünme becerilerini, teorik matematik, yazılım, finans ve yönetim matematiği, biyomatematik, veri bilimi ve finansal istatistik yöntemleri gibi disiplin-İçi ve disiplinlerarası uzmanlık alanlarında geliştirebileceklerdir. / Advance their acquired knowledge in mathematics and mathematical thinking skills in both disciplinary and interdisciplinary areas of specialisation such as pure mathematics, software, financial and managerial mathematics, biomathematics, data science, and financial statistical methods.	=	=	=	=	=	=
PC-6 Matematik alanında yaygın olarak kullanılan en az bir programlama dili ile bilgisayar ve yapay zekâ teknolojilerini, problemleri çözmek, veri analizi yapmak ve simülasyonlar gerçekleştirmek için kullanabileceklerdir. / Use at least one programming language and computer and artificial intelligence technologies widely employed in mathematics for problem-solving, data analysis, and simulations.	=	=	=	=	=	=
PC-7 Matematik ve ilgili alanlardaki bilimsel ve teknolojik gelişmeleri izleyebilecek, kariyer fırsatlarını değerlendirerek kişisel ve mesleki gelişim hedeflerini belirleyebilecek ve bu hedeflere ulaşmak için hayat boyu öğrenme stratejilerini kullanabileceklerdir. / Follow scientific and technological developments in mathematics and related fields, assess career opportunities, identify personal and professional development goals, and adopt lifelong learning strategies to achieve these goals.	=	=	=	=	=	=
PC-8 Bilimsel araştırmalarını ve mesleki faaliyetlerini yürütürken doğabilecek hukuksal sonuçları ve toplumsal etkileri dikkate alarak mesleki etik ilkeler, kalite standartları ile evrensel değerler doğrultusunda ve sosyal sorumluluk bilinci ve adalet duygusuyla hareket edebileceklerdir. / Act with a sense of social responsibility and justice and in accordance with professional ethical principles, quality standards, and universal values by taking into account potential legal and societal	=	=	=	=	=	=



consequences of their scientific research and professional activities.						
PC-9 Bireysel olarak ya da takımlarda etkin biçimde çalışabileceklerdir. / Work effectively both independently and as part of a team.	<u>3</u>	<u>3</u>	<u>3</u>	<u>3</u>	<u>3</u>	<u>3</u>
PC-10 Matematik alanında güvenilir bilgi kaynaklarına ulaşarak literatür taraması yapabilecek ve akademik araştırma tasarlayıp yürütebileceklerdir. / Access reliable sources of information, conduct literature reviews, and design and carry out academic research in the field of mathematics.	=	=	=	=	=	=
PC-11 Matematiksel konuları, teorileri, ispatları, araştırmaları ve problem çözümlerini, matematik terminolojisi kullanarak tüm paydaşlara Türkçe ve İngilizcede sözlü ve yazılı olarak etkili biçimde aktarabileceklerdir. / Effectively communicate mathematical topics, theories, proofs, research, and problem solutions to all relevant stakeholders using appropriate mathematical terminology, both orally and in writing, in Turkish and in English.	=	=	=	=	=	=