ISTANBUL GELISIM UNIVERSITY

COURSE CATALOGUE

Course Name				Criptology		
Code	Semester	Local Credits	ECTS Credits	Course Implementation, Hours/Week		
				Theoretical	Tutorial	Laboratory
BIL423	5	3	6	3	0	0

Department/Program	Computer Eng./ Computer Eng.		
Course Type	Elective	Course Language	Turkish
Course Prerequisites	None		

Course Category by Content, %	Basic Sciences	Engineering Science	Engineering Design	General Education
	%10	%50	%30	%10

Course Description	Basic concepts of encryption, encryption systems, algorithms, operating principles, encryption standards, public and private encryption types, digital signature and network security techniques.
Course Objectives	To teach the students the requirements of the encryption concept considering historical development, the operating structure of the most widely used encryption (crypto) systems and their use in today's encryption systems.
Course Learning Outcomes	The students who take the course will be able to I. Recognizes the basic concepts and logic of encryption. II. Have knowledge about modern Symmetric and Asymmetric passwords. III. Makes cryptology applications. IV. Uses cryptology algorithms.
Textbook	Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar and Jan Pelzl Springer, 1st Edition, 2010
Other References	Introduction to Computer Security - M. T. Goodrich and R. Tamassia, 2011 | Pearson Prentice Hall | ISBN-13: 978-0-321-70201-2, ISBN-10
Homework & Projects	Yes
Laboratory Work	None
Computer Use	Yes
Other Activities	None

Assessment Criteria	Activities	Quantity	Effects on Grading, %
	Midterm Exam	1	%30
	Quizzes	2	%10
	Homework	2	%10
	Projects		
	Term Paper/Project		
	Laboratory Work		
	Other Activities		
	Final Exam	1	%50

Course Plan

Weeks	Topics	Course Outcomes
1	Introduction To Cryptography	I
2	Stream Ciphers	I-II
3	The Data Encryption Standard (Des)	I-II
4	The Advanced Encryption Standard (Aes)	I-II
5	More About Block Ciphers	I-II
6	Introduction To Public-Key Cryptography	I-II
7	The Rsa Cryptosystem	I-II
8	Mid-Term Exam	
9	Public-Key Cryptosystems Based On The Discrete Logarithm Problem	I-II
10	Elliptic Curve Cryptography	I-II-III
11	Digital Signatures	I-II-III
12	Hash Functions	I-II-III-IV
13	Message Authentication Codes (Macs)	I-II-III-IV
14	Key Establishment, Encryption Current Technological Developments And Events	I-II-III-IV
15	Cryptography Overview	I
16	Final Exam	
17	Final Exam	

Relationship between the Course and Program

Program Outcomes		Contribution
1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics	X
2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors	X
3	an ability to communicate effectively with a range of audiences	
4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts	
5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives	
6	an ability to develop and conduct appropriate experimentation, analyze, and interpret data, and use engineering judgment to draw conclusions	X
7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies	X

Lecturer	Assist.Prof. Serkan GÖNEN
Date	

İSTANBUL GELİŞİM ÜNİVERSİTESİ

DERS KATALOĞU

Dersin Adı				Şifreleme		
Kodu	Yarıyılı	Kredisi	AKTS Kredisi	Ders Dağılımı, Saat/Hafta		
				Teorik	Uygulama	Laboratuvar
BIL423	5	3	6	3	0	0

Bölüm/Program	Bilgisayar Mühendisliği/Bilgisayar Mühendisliği		
Dersin Türü	Seçmeli	Dersin Dili	Türkçe
Dersin Önkoşulları	Yok		

Dersin İçeriğe Göre Kategorisi %	Temel Bilim	Temel Mühendislik	Mühendislik Tasarımı	İnsan ve Toplum Bilim
	%10	%50	%30	%10

Dersin İçeriği	Şifreleme ile ilgili temel kavramlar, temel şifreleme sistemleri, algoritmaları, çalışma prensipleri şifreleme standartları, açık ve gizli şifreleme türleri, sayısal imza ve ağ güvenliği teknikleri.
Dersin Amacı	Öğrencilere, şifreleme konseptinin gereklerini tarihsel gelişim dikkate alınarak verilmesi, en yaygın kullanılan şifreleme (kripto) sistemlerinin çalışma yapısını ve günümüz şifreleme sistemlerinde kullanımını öğretmektir.
Dersin Öğrenme Çıktıları	Bu dersi alan öğrenciler şu kabiliyetleri kazanırlar; I. Şifreleme temel kavramlarını ve mantığını tanır. II. Modern Simetrik ve Asimetrik şifreler hakkında bilgi sahibi olur. III. Şifreleme uygulamalarını yapar. IV. Şifreleme algoritmaları kullanır.
Ders Kitabı	Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar and Jan Pelzl Springer, 1st Edition, 2010
Diğer Kaynaklar	Introduction to Computer Security - M. T. Goodrich and R. Tamassia, 2011 | Pearson Prentice Hall | ISBN-13: 978-0-321-70201-2, ISBN-10
Ödevler ve Projeler	Var
Laboratuvar Uygulamaları	Yok
Bilgisayar Kullanımı	Var
Diğer Uygulamalar	Yok

Başarı Değerlendirme Sistemi	Faaliyetler	Sayısı	Değerlendirmedeki Katkısı, %
	Yıl İçi Sınavları	1	%30
	Kısa Sınavlar	2	%10
	Ödevler	2	%10
	Projeler		
	Dönem Ödevi/Projesi		
	Laboratuvar Uygulaması		
	Diğer Uygulamalar		
	Final Sınavı	1	%50

Ders Planı

Hafta	Konular	Dersin Çıktıları
1	Şifrelemeye Giriş	I
2	Akış Şifreleri	I-II
3	Veri Şifreleme Standardı (The Data Encryption Standard-Des)	I-II
4	Gelişmiş Şifreleme Standardı (The Advanced Encryption Standard-Aes)	I-II
5	Blok Şifreleme	I-II
6	Açık Anahtarlı Kriptografiye Giriş	I-II
7	Rsa Şifreleme Sistemi	I-II
8	Ara Sinav	
9	Ayrık Logaritma Problemine Dayalı Açık Anahtarlı Şifreleme Sistemleri	I-II
10	Eliptik Eğri Şifreleme Sistemleri	I-II-III
11	Dijital Imzalar	I-II-III
12	Hash Fonksiyonları	I-II-III-IV
13	Mesaj Kimlik Doğrulama Kodları	I-II-III-IV
14	Anahtar Dağıtım, Şifreleme Güncel Teknolojik Gelişmeler Ve Yaşanan Olaylar	I-II-III-IV
15	Genel Konu Tekrarları	I
16	Final	
17	Final	

Dersin Programla İlişkisi

Programın mezuna kazandıracağı bilgi ve beceriler (Programa ait çıktılar)		**Katkı**
1	Mühendislik, bilim ve matematik ilkelerini uygulayarak karmaşık mühendislik problemlerini tanımlama, formüle etme ve çözme becerisi	X
2	Halk sağlığı, güvenliği ve refahının yanı sıra küresel, kültürel, sosyal, çevresel ve ekonomik faktörleri dikkate alarak belirli ihtiyaçları karşılayan çözümler üretmek için mühendislik tasarımını uygulama becerisi	X
3	Çeşitli izleyicilerle etkili iletişim kurma becerisi	
4	Mühendislik durumlarında etik ve profesyonel sorumlulukları tanıma ve mühendislik çözümlerinin küresel, ekonomik, çevresel ve toplumsal bağlamlardaki etkisini dikkate alması gereken bilgiye dayalı kararlar verme becerisi	
5	Üyelerinin birlikte liderlik sağladığı, işbirlikçi ve kapsayıcı bir ortam yarattığı, hedefler belirlediği, görevleri planladığı ve hedefleri karşıladığı bir ekipte etkin bir şekilde çalışabilme becerisi	
6	Uygun deneyler geliştirme ve yürütme, verileri analiz etme ve yorumlama ve sonuçlara varmak için mühendislik yargısını kullanma becerisi	X
7	Uygun öğrenme stratejilerini kullanarak gerektiğinde yeni bilgi edinme ve uygulama becerisi	X

Dersi Veren Öğretim Üyesi	Dr.Öğr.Üyesi Serkan GÖNEN
Tarih	