ORTA DOĞU TEKNİK ÜNİVERSİTESİ
UYGULAMALI MATEMATİK ENSTİTÜSÜ

RAPOR
2007

INSTITUTE OF APPLIED MATHEMATICS
MIDDLE EAST TECHNICAL UNIVERSITY
ODTÜ ANKARA 06531
Tel: +90 (312) 210 29 87
Fax: +90 (312) 210 29 85
http: //www.iam.metu.edu.tr
E-mail: wwwiam@metu.edu.tr

İÇİNDEKİLER

ÖNSÖZ.....2
ÖZET BİLGİLER.....4
ENSTİTÜNÜN PROGRAMLARI.....5
İNSAN KAYNAKLARI.....5
PROTOKOLLER.....7
ÖĞRENCİ BİLGİLERİ.....8
ARAŞTIRMA FAALİYETLERİ.....11
YAYINLAR/TEBLİĞLER*.....11
ÇALIŞTAY/ SEMPOZYUM/ KONFERANS/ YAZOKULU.....17
ARAŞTIRMA GRUPLARI/ DOSAP PROGRAMI.....18
YÜRÜTÜCÜLÜĞÜ YAPILAN PROJELER.....20
DİĞER FAALİYETLER.....24
EKLER.....27

ÖNSÖZ

Orta Doğu Teknik Üniversitesi'nde Uygulamalı Matematik Enstitüsü kurulması; Milli Eğitim Bakanlığı'nın 8/5/2002 tarihli ve 12293, 12296 sayılı yazıları, 28/3/1983 tarihli ve 2809 sayılı kanunun değişik ek 30. maddesine göre, Bakanlar Kurulu'nca 16/5/2002 tarihinde kararlaştırılmıştır ve bu karar 21 Haziran 2002 tarihinde resmi gazetede yayınlanmıştır. Enstitü eğitim faaliyetlerini Kriptografi, Bilimsel Hesaplama, Finansal Matematik, ve Finansal Matematik Hayat Sigortası Opsiyonu programları ile aşağıdaki misyonlar çerçevesinde sürdürmektedir:

I. Orta Doğu Teknik Üniversitesi'nin araştırma potansiyeli ve ülkemizin ihtiyaçları göz önüne alınarak, disiplinler arası matematik bazlı araştırma/uygulama alanları belirlemek ve bu çerçevede lisansüstü eğitim programlarını geliştirmek. Üniversitemizde yapılmakta olan matematik ağırlıklı araştırmaları koordine ederek Enstitü bünyesinde disiplinler-arası bir çalışma ortamı oluşturmak, bu alanlarda araştırmaya yönelik konferanslar/yaz okulları düzenlemek ve uluslararası işbirliği olanaklarını araştırmak/hayata geçirmek.

II. Matematiğin; doğayı, teknolojik ve ekonomik süreçleri daha iyi anlama yolunda bilim adamlarının ortak dili olduğundan hareketle, lisans/lisansüstü eğitimde ve araştırmalarda matematik kullanımının hem nicelik hem de nitelik açısından arttırılması yolunda çalışmalarda bulunmak, bu çerçevede yeni, uygulanabilir matematik konularında araştırmacıları bilgilendirmek ve bu amaca yönelik araştırmalar yapmak.

III. Uygulamalı matematik alanında ODTÜ-Sanayi/Kamu kuruluşları işbirliğini, gerek proje ve ürün geliştirerek gerekse kısa süreli eğitim/araştırma toplantıları düzenleyerek hayata geçirmek.

Bu rapor Uygulamalı Matematik Enstitüsü'nün misyonu çerçevesinde 01.01.2007-31.12.2007 tarihleri arasındaki faaliyetleri içermektedir.

Enstitü Yönetimi

Müdür

Prof. Dr. Ersan AKYILDIZ

Müdür Yardımcıları

Y. Doç. Dr. İlkay ULUSOY(1)

Y. Doç. Dr. Işıl EROL

Enstitü Kurulu(2)

Prof. Dr. Ferruh ÖZBUDAK(3)

Prof. Dr. Bülent KARASÖZEN

Enstitü Yönetim Kurulu(2)

Prof. Dr. Haluk AKSEL

Y. Doç. Dr. Seza DANIŞOĞLU

Prof. Dr. Mete SEVERCAN

(1) Y. Doç. Dr. Yusuf ULUDAĞ, Enstitü Müdür Yardımcılığı görevinden 1 Ekim 2007 tarihinde ayrılmış yerine Y. Doç. Dr. İlkay Ulusoy atanmıştır.
(2) Enstitü Yönetimi, bu kurulların doğal üyeleridir.
(3) Prof. Dr. Rüyal ERGÜL Kriptografi EABD Başkanlığından 15.3. 2007 tarihinde ayrılmış yerine Prof. Dr. Ferruh ÖZBUDAK atanmıştır.

ÖZET BİLGİLER

- Enstitünün 2007 yılı faaliyetlerine 5 UME, 36 ODTÜ içi, 15 ODTÜ dışı bağlantılı öğretim üyesi katkıda bulunmuşlardır.
- Enstitümüzde toplam 14 araştırma görevlisi vardır, bunların 10'u Öğretim Üyesi Yetiştirme Programı (ÖYP) ve biri de 35. madde kapsamında görev almaktadır. Bir asistanımız ise Amerika Birleşik Devletleri Florida State Üniversitesi'nde YÖK burslusu olarak çalışmalarını sürdürmektedir.
- Enstitümüzde toplam 165 öğrenci eğitimini sürdürmektedir. Bu öğrencilerin 26'sı Bilimsel Hesaplama, 69'u Finansal Matematik, 70'i ise Kriptografi programındadır.
- Erasmus programı çerçevesinde 5 öğrencimiz değişik üniversitelere gitmiştir.
- Enstitümüz anabilim dallarının 11 araştırma grubu bulunmaktadır.
- Enstitü bağlantısı belirtilmiş olarak 10 yurtdışı yayın, 8 yurtdışı ve 14 yurtiçi tebliğ, 36 yurtdışı ve 18 yurtiçi sunum yapılmış, 1 yurtdışı kitapta makale ve 1 yurtiçi kitap çıkarılmıştır.
- Enstitümüz tarafından düzenlenen bilimsel toplantılar:
  - "Bilgi Güvenliği ve Kriptoloji Konferansı", Ankara
  - "Workshop on Sustainable Living at Turkish Rural Countryside", Ankara
  - "EURO-CBBM Workshop - Workshop on OR in Computational Biology, Bioinformatics and Medicine", Çekoslovakya
  - "EURO XXII 2007", Çekoslovakya
- Ensitümüz ile Max-Planck Institute (Germany) ve Universtiy of Ballarat (Australia) arasında iki protokol yürürlüğe girmiştir.
- Enstitümüz öğretim üyeleri tarafından yürütücülüğü yapılan 18, araştırmacı olarak katıldıkları ise 5 proje bulunmaktadır.
- Dr. Ali Devin Sezer, öğretim görevlisi olarak enstitüde göreve başlamıştır.
- Enstitümüzü yurtdışından 16 öğretim üyesi ziyaret ederken, 5 öğretim elemanı da enstitümüz tarafından desteklenerek yurt dışında görevlendirilmiştir.
- Finansal Matematik anabilim dalı başkanımız Prof. Dr. Hayri Körezlioğlu vefat etmiştir.
- Kriptografi EABD Başkanlığına Prof. Dr. Ferruh ÖZBUDAK atanmıştır.
- Müdür Yardımcılığı görevine Y. Doç. Dr. İlkay Ulusoy atanmıştır.

ENSTİTÜNÜN PROGRAMLARI

Bilimsel Hesaplama
Tezli Yüksek Lisans
Doktora

Finansal Matematik
Tezli Yüksek Lisans
Tezsiz Yüksek Lisans
Doktora

Kriptografi
Tezli Yüksek Lisans
Tezsiz Yüksek Lisans
Doktora

Finansal Matematik Hayat Sigortası Opsiyonu
Tezsiz Yüksek Lisans

İNSAN KAYNAKLARI

Öğretim Elemanları
Prof. Dr. Gerhard- Wilhelm Weber
Y. Doç. Dr. Hakan Öktem
Y. Doç. Dr. Emrah Çakçak
Dr. Ali Devin Sezer
Dr. Ömür Uğur

DOSAP
Y. Doç. Dr. Pakize Taylan*
(Dicle Üniversitesi)
Y. Doç. Dr. Nedim Dikmen*
(Giresun Üniversitesi)

Araştırma Görevlileri
Sedat Akleylek (ÖYP, Samsun)
Derya Altıntan (ÖYP, Konya)
Derviş Bayazıt (YÖK Bursu ile yurtdışında)
Canan Çimen
Zehra Ekşi**
Nüket Erbil (ÖYP, Elazığ)
Zeynep Sırma Alparslan Gök (ÖYP, Isparta)
İ. Ethem Güney
Rita İsmailova (ÖYP, Kırgızistan)
Ayşegül İşcanoğlu (ÖYP, Konya)
Turgut Hanoymak (ÖYP, Van)
Barış Bülent Kırlar (ÖYP, Isparta)
Süreyya Özöğür**
Ayşe Sarıaydın (ÖYP, Van)
Zülfükar Saygı**
Nurbek Baryk Ulu (ÖYP, Kırgızistan)
Enes Yılmaz (35. madde)

*2007 yılı içinde üniversitelerine dönmüşlerdir.

**2007 yılı içinde araştırma görevliliğinden ayrılmışlardır.

BAĞLANTILI ÖĞRETİM ÜYELERİ

ORTA DOĞU TEKNİK ÜNİVERSİTESİ

Matematik Bölümü	Marat U. Akhmet Ersan Akyıldız Muhammed Dabbagh Ali Doğanaksoy Bülent Karasözen Ferruh Özbudak Münevver Tezer Muhiddin Uğuz
Elektrik-Elektronik Mühendisliği Bölümü	Yeşim Serinağaoğlu Doğrusöz F. Rüyal Ergül Nevzat G. Gençer Kemal Leblebicioğlu Osman Sevaioğlu Mete Severcan İlkay Ulusoy Melek Yücel
İşletme Bölümü	Nuray Güner Adil Oran Seza Danışoğlu Rhoades
İktisat Bölümü	Işıl Erol Esma Gaygısız Şaziye Gazioğlu
Biyoloji Bölümü	Meryem Beklioğlu Semra Kocabıyık İnci Togan
İstatistik Bölümü	Ayşen Akkaya B. Burçak Başbuğ İnci Batmaz
Gıda Müh.Bl.	Zümrüt Begüm Ögel
Endüstri Müh. Bl.	Gülser Köksal
Kimya Bölümü	Ali Gökmen
Kimya Müh. Bl.	Yusuf Uludağ Gürkan Karakaş
Beden Eğitimi ve Spor Bl.	Feza Korkusuz
Enformatik Enstitüsü	Erkan Mumcuoğlu
Makine Müh. Bl.	Haluk Aksel

ÜNİVERSİTELER

ANKARA ÜNİV. **İstatistik Bölümü**	Ömer Gebizlioğlu
ATILIM ÜNİV. **Matematik Bölümü**	Tanıl Ergenç
DOĞUŞ ÜNİV. **Matematik Bölümü**	İsmail Güloğlu
HACETTEPE ÜNİV. İstatistik Bölümü	Gül Ergün
ALBERT-LUDWIGS UNIVERSITY FREIBURG Department of Economics	Sevtap Selçuk Kestel
İZMİR YÜKSEK TEKNOLOJİ ENSTİTÜSÜ **Matematik Bölümü**	Ali İhsan Neslitürk
KOÇ ÜNİV. **Mühendislik Fakültesi**	Metin Türkay
KIRIKKALE ÜNİV. **İstatistik Bölümü**	Fatih Tank
OREGON STATE UNİV.	Çetin Kaya Koç
TRAKYA ÜNİV. **İktisat Bölümü**	Kasırga Yıldırak
TOBB-ETU **Matematik Bölümü**	Zülfükar Saygı
UNIV. OF SOUTH ALABAMA	Can Akkoç

KURUMLAR

TCMB	C.Coşkun Küçüközmen
TÜBİTAK-UEKAE	Orhun Kara
DİĞER	Azize Hayfavi

İDARİ PERSONEL

Sekreter	Nejla Erdoğdu Rukiye Ekinci Figen Pekmez
Memur	M. Kemal Yaşar
TÜBİTAK-KAMU Proje Elemanı	Burçin Ak
İdari Amir	Saffet Aykın
Görevli	Muharrem Kayabel Serkan Demiröz

PROTOKOLLER

Universitat Kaiserslautern (Germany) and Middle East Technical University	Cooperation in the Field of Financial and Insurance Mathematics at Institute of Applied Mathematics
- The Institute of Mathematics "Siroion Stoiow" of the Romainan, Academy (IMAR)-Romania **- The Institute of Mathematical Statistics and Applied Mathematics "Gheorghe Mihoc-Caius Iacob (ISMMA)-Romania** **- The Institute of Applied Mathematics and Department of Mathematics**	Cooperation in the fields of Financial Mathematics, and Cryptography
University of the Aegean (Greece) and Middle East Technical University	Cooperation in the fields of Financial Mathematics, Actuarial Sciences and Establishment of a Joint Doctoral Program at Institute of Applied Mathematics
The Institute of Mathematics of The Polish Academy of Sciences (Poland) and Institute of Applied Mathematics and Department of Mathematics	Memorandum on Extending and Strengthening Links Beetween Polish Academy of Sciences and the Department of Mathematics and Institute of Applied Mathematics
Laboratoire de Mathématiques et Applications Université de La Rochelle (France) and Institute of Applied Mathematics	Turkish-French University and Scientific Cooperation Projects: Exchange of know-how in Financial Mathematics, Development of common teaching and research programs, Joint participation to European research projects.
University of Ballarat, (Australia) and Middle East Technical University	Collaboration between the Centre for Informatics and Applied Optimization, University of Ballarat Australia, and the Institute of Applied Mathematics, the Middle East Technical University, Turkey.
Telekomünikasyon Kurumu- ODTÜ	Bilgi ve İletişim Teknolojileri Konularında Eğitim, Araştırma, Geliştirme Çalışmaları ve Uygulamalarında İşbirliği Yapılması, yürütücü, Uygulamalı Matematik Enstitüsü Müdürlüğü, ODTÜ
- MPI for Mathematics in the Sciences, Research Group on Complex Systems, Leipzig (Australia) **- Interdisciplinary Center for Bioinformatics, University of Leipzig (Australia)** **- The Institute of Applied Mathematics** **- CAS-MPG Partner Institute for Computational Biology, Shanghai (China)** **- Koç University** **- Işık University**	Collaboration in the fields of mathematical modeling of biological networks, network dynamics and information processing, algebraic structure of graphs and discrete and continuous optimization problems in computational biology.

ÖĞRENCİ BİLGİLERİ

SIAM-IAM ODTÜ ÖĞRENCİ TOPLULUĞU

SIAM (Society of Industrial and Applied Mathematics) IAM (ODTÜ) Öğrenci Topluluğu; Uygulamalı Matematik Enstitüsü'nün çalışmaları sonucu Amerika ve Kanada dışında kurulan ilk SIAM öğrenci grubudur. Grubun amaçları, SIAM'ı ve SIAM'ın faaliyetlerini Üniversite'de ve Türkiye'de tanıtmaktır. Mathematics Awareness Month 2007 çerçevesinde "Mathematics and Brian" konusunda 25 Mayıs 2007 tarihinde Nurgul Gökgöz, Serdar Tanıl ve Ahmet Onur **"**Iterative Methods for Discrete Tomography Implementation & Comparison Kaczmarz's Method and Conjugate Gradient Least Squares Method" ve Neslihan Özmen, Fatma Yerlikaya, Doğa Gürsoy "The Inverse Problem of Magnetoencepkulography: Sourse Localization and The Shape of Ball" başlıklı sunumlar yapılmıştır. Grup hakkında ayrıntılı bilgi www.siam.metu.edu.tr adresinde verilmiştir.

ERASMUS PROGRAMI

Finansal Matematik	Orçun Kaya	Kopenhag University	I Dönem
Finansal Matematik	Burak Yıldırım	Kopenhag University	I Dönem
Finansal Matematik Hayat Sigortası Opsiyonu	İlkin Menet	University of Tilburg	I Dönem
Finansal Matematik Hayat Sigortası Opsiyonu	Raşit Özkan	Chemnizt Universty	I Dönem
Kriptografi	Deniz Toz	Katholieke University Leuven	I Dönem

Enstitümüzün Toplam Öğrenci Sayısı: 165

2007 yılında Kayıt Yaptıran Öğrenci Sayısı: 58

2007 Yılında Mezun Olan Öğrenci Sayısı*:18

Yüksek Lisans Tezli	Yüksek Lisans Tezsiz	Doktora
10	6	2

* Bu öğrencilerin listesi **Ek 4**'de verilmiştir.

BAŞVURULAR

	2007-2008		
	BAŞVURU	**KABUL**	**KAYIT**
Bilimsel Hesaplama	24	14	12
Finansal Matematik	62	35	23
Hayat Sigortası	10	6	0
Kriptografi	40	26	23
Toplam	**136**	**81**	**58**

Enstitümüz Öğrencilerinin Programlara göre Dağılımı

Anabilim Dalı	**Yüksek Lisans**	**Doktora**	**Bilimsel Hazırlık**	**İngilizce Hazırlık**
Bilimsel Hesaplama **(26)**	**14**	**11**	**-**	**1**
Finansal Matematik **(63)**	**36**	**17**	**10**	**-**
Finansal Matematik **(6)** Hayat Sigortası Opsiyonu	**6**	**-**	**-**	**-**
Kriptografi **(70)**	**33**	**34**	**3**	**-**
Toplam: **(165)**	**89**	**62**	**13**	**1**

2007 yılında Kayıt Yaptıran Öğrencilerin B.S. Derecelerini Aldıkları Bölümlere Göre Dağılımları*

MATH	ECON	STAT	CENG	IE	BA	AEE	EE	STPS	ME
28	**8**	**6**	**5**	**4**	**2**	**2**	**1**	**1**	**1**

UME Derslerini Alan Öğrencilerin Bölümlere Göre Dağılımı**

Dönem	**UME**	**MATH**	**EE**	**BIOL**	**CE**	**CHE**	**CHEM**	**GGIT**	**IS**	**CENG**	**ECON**	**IE**	**STAT**	**METE**	**ENVE**	**MI**	**AEE**	**BME**	**BA**	**SSME**	**Özel Öğr.**	**TOTAL**
2006-2007 II	**204**	**14**	**6**	**-**	**1**	**1**	**-**	**-**	**2**	**-**	**2**	**-**	**-**	**1**	**-**	**2**	**-**	**1**	**-**	**1**	**6**	**241**
2007-2008 I	**235**	**3**	**1**	**2**	**2**	**-**	**-**	**1**	**-**	**6**	**5**	**4**	**2**	**-**	**-**	**1**	**3**	**2**	**1**	**-**	**12**	**280**

*Bölüm isimlerinde ODTÜ Katalogunda ki kısaltmalar kullanılmıştır.
** Enstitümüzde 2006-2007 II ve 2007-2008 I. Döneminde verilen derslerin listesi **Ek 6**'da verilmektedir.

Dönemsel Ders İstatistikleri:

	Verilen Ders Sayısı	Toplam Öğrenci Sayısı	Ders Başına Verilen Not Sayısı
2006-2007 II.Dönem	20	241	12
2007-2008 I.Dönem	23	280	12

Öğrenci Başarı Durumları

	2006-2007 II.Dönem				2007-2008 I.Dönem			
	Başarılı	**Başarısız**	**İlişiği Kesilen**	**İzinli**	**Başarılı**	**Başarısız**	**İlişiği Kesilen**	**İzinli**
Kriptografi (Bil.Haz.)	-	-	-	-	3	-	-	-
Kriptografi (M.Sc.)	16	7	1	1	22	8	3	-
Kriptografi (Ph.D.)	27	3	1	2	31	1	-	2
Bilimsel Hesaplama (İng. Haz.)	-	-	-	-	1	-	-	-
Bilimsel Hesaplama (M.Sc.)	9	2	-	1	10	3	1	-
Bilimsel Hesaplama (Ph.D.)	8	-	-	-	11	-	-	-
Finansal Matematik (Bil. Haz.)	-	1	-	-	1	9	-	-
Finansal Matematik (İng. Haz.)	1	-	-	-	-	-	-	-
Finansal Matematik (M.Sc.)	21	7	-	-	23	13	-	-
Finansal Matematik (Ph.D.)	10	-	-	4	11	2	-	4
Hayat Sigortası (M.Sc.)	3	5	-	-	4	2	-	-
TOPLAM	**95**	**25**	**2**	**8**	**117**	**38**	**4**	**6**

ÖYP Öğrencileri Başarı Durumları

	Bilimsel Hesaplama			Finansal Matematik			Kriptografi					
Üniversitesi	YL	Doktora	LSD	YL	Doktora	LSD	YL	Doktora	LSD	Başarılı	Başarısız	Mezun
Selçuk Üniversitesi KONYA	-	1	-	-	1	-	-	-	-	2	-	-
Süleyman Demirel Üniversitesi ISPARTA	-	-	1	-	-	-	-	1	-	2	-	-
Yüzüncü Yıl Üniversitesi VAN	-	-	-	-	-	-	-	-	1	1	-	-
Fırat Üniversitesi ELAZIĞ	-	-	-	1	-	-	-	-	-	1	-	-
Ondokuz Mayıs Üniversitesi SAMSUN	-	-	-	-	-	-	1	-	-	1	-	-
Kırgız Milli Üniversitesi	-	-	-	-	-	-	1	-	-	-	1	-
Kırgız Türkiye Manas Üniversitesi	-	-	-	-	-	-	-	1	-	1	-	-

ARAŞTIRMA FAALİYETLERİ

YAYINLAR/TEBLİĞLER*

Yurtdışı Yayın	Yurtdışı Tebliğ	Yurtdışı Konferanslarda Sunum
12	**6**	**38**

YURTDIŞI YAYINLAR

- **E. Çakçak, F. Özbudak,** "Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places", Journal of Pure and Applied Algebra, vol. 210, no. 1, pp. 113-135, 2007.
- **A. Aydın, B. Karasözen,** Symplectic and multi-symplectic methods for coupled Nonlinear Schrödinger Equations with periodic solutions, Computer Physics Communications, 177, 566-583, 2007.
- **B. Karasözen,** "Survey of Trust-region Derivative Free Optimization Methods", Journal of Industrial and Management Optimization, 3, 321-334, 2007.
- **M.U.Akhmet,** "On the Reduction Principle for Differential Equations with Piecewise Constant Argument of Generalized", Journal of Mathematical Analysis and Applications, 336, 646-663, 2007.
- **M.U. Akhmet,** "Integral Manifolds of Differential Equations with Piecewise Constant Argument of Generalized Type", Nonlinear Analysis: Theory, Methods and Applications, 66, 367-383, 2007.
- **M.U. Akhmet, M. Tleubergenova, A. Zafer, "**Asymptotic Equivalence Of Differential Equations And Asymptotically Almost Periodic Solutions**,** Nonlinear Analysis: Theory, Methods and Applications, 67, 1870-1877, 2007.
- **J. Gebert, N. Radde, G.-W. Weber, "**Modeling Gene regulatory networks with piecewise linear differential equations**", European Journal of Operational Research 181, 1148-1165, 2007.**
- **Ö. Uğur and G.-W. Weber,** "Optimization and Dynamics of Gene-Environment Networks with Intervals", in the special issue in honour of Prof. Dr. Alexander Rubinov of Journal of Industrial and Management Optimization (JIMO) 3, 2, 357-379, 2007.
- **P. Taylan, G.-W. Weber, A. Beck,** "New Approaches to Regression by Generalized Additive Models and Continuous Optimization for Modern Applications in Finance", science and techology, to appear in the special issue in honour of Prof. Dr. Alexander Rubinov, of Optimization 56, 5-6, 675-698, 2007.
- **G.-W. Weber, P. Taylan, B. Akteke-Öztürk, Ö. Uğur**, "Mathematical and Data Mining Contributions to Dynamics and Optimization of Gene-Environment Networks", invited paper, in the special issue; Interdisciplinary Applications in Physics: Complexity in Social and Biological Systems of Electronic Journal of Theoretical Physics (EJTP) 4, 16(II), 115-146, 2007.
- **P. Taylan and G.-W. Weber,** "New approaches to regression in financial mathematics by additive models", Journal of Computational Technologies 12, 2, 3-22, 2007.
- **G.-W. Weber, A. Tezel,** "On Generalized Semi-infinite Optimization of Genetic Networks", TOP 15, 1, 65-77, 2007.

* Tüm araştırma faaliyetlerinde sadece UME bağlantılarını belirtmiş öğretim üyelerimizin faaliyetleri dikkate alınmıştır. Bu faaliyetlerinn listesi **Ek 1**'de verilmektedir

YURTDIŞI TEBLİĞLER

- **M. Sönmez Turan, "**A Framework for Chosen IV Statistical Analysis of Stream Ciphers", Progress in Cryptology-INDOCRYPT 2007, vol. 4859 of Lecture Notes of Computer Science, 268-281, Springer-Verlag, 2007.
- **A. Doğanaksoy, E. Saygı, Z. Saygı,** "Quadratic Feedback Shift Registers Generating Maximum Length Sequences", International Conference on Boolean Functions: Cryptography and Applications, BFCA'07, Paris, France, May 2-3, 2007.
- **F. Özbudak, Z. Saygı,** "Constructions of systematic authentication codes using additive polynomials", Proceedings of International Workshop on Coding ad Cryptography 2007, Versailles, France, pp. 405-414, 2007.
- **E. Akkemik, O. Kara, C. Manap,** "Success Rate of Reflection Attack on Some DES Variants", International Conference on Security of Information and Networks (SIN 2007), Salamis Bay Conti Resort Hotel, Gazimagusa (TRNC), North Cyprus, Trafford Publishing, IX+370 pages, pp 136-145, May 8-10, 2007.
- **M. Taştan, Ö. Çelik, G.-W. Weber, F. Korkusuz, B. Karasözen,** "New Approaches in Mathematical Modeling of Proximal Femur Geometry and Bone Mineral Density", International Symposium on Health Informatics and Bioinformatics Turkey '07, HIBIT, Antalya, Turkey, (http://hibit.ii.metu.edu.tr/07/index.html) April 30 - May 2, 2007.
- **G.-W. Weber, Ö. Uğur,** "Optimizing Gene-Environment Networks: Generalized Semi-infinite Programming Approach with Intervals", in the proceedings of International Symposium on Health Informatics and Bioinformatics Turkey '07, HIBIT, Antalya, Turkey, (http://hibit.ii.metu.edu.tr/07/index.html) April 30 - May 2, 2007.

ULUSLARARASI KONFERANSLARDA SUNUMLAR

- **A. İşcanoğlu, G.-W. Weber, P. Taylan**, Predicting Default Probabilities with Generalized Additive Models for Emerging Markets, 22 European Conference on Operational Research, EURO Prag, 8-11 July 2007.
- **M. Sönmez Turan, O. Kara,** "Linear Approximations for 2-round Trivium", SASC07 Stream Ciphers Revisited, Bochum, Germany 2007.
- **M. Sönmez Turan, O. Kara**, "Linear Approximations for 2-round Trivium", International Conference on Security of Information and Networks, Cyprus, 2007.
- **A. Doğanaksoy, O. Özen, K. Varıcı**, "On the Security of the Encryption Mode of Tiger", Tools for Cryptanalysis, Poland, 2007.
- **S. Akleylek, L. Emmungil**, "Accessibility and Usability of E-government Web-Sites of Social Security Foundations", 3th International Conference on Information Technologies and Telecommunication, Azerbaijan, October 4-6 2007.
- **E. Akyıldız,** "Elliptic Curves in Cryptography", International Conference on Security of Information and Networks (SIN 2007), Cyprus, 8-10 May 2007.
- **E. Akyıldız,** "Elliptic Curves in Cryptography", Projective Geometry and Commutative Algebra in Applications, Italy, June 15-16, 2007.
- **L. Emmungil, S. Akleylek**, **U. Nuriyev**, "Security Analysis and Proposed Solutions About Wireless Campus Networks of Universities in Turkey", 3th International Conference on Information Technologies and Telecommunication, Azerbaijan, October 4-6 2007.
- **M. Akhmed**, "On the compartmental model of blood pressure distribution", Fifth International Conference on Dynamical Systems and Applications, Atlanta, USA, 28 May-4 June, 2007.
- **G.-W. Weber, S. Z. Alparslan Gök, M. U. Akhmet, S. Pickl**, "A New Mathematical Approach in Environmental Protection: Gene-Environment Networks and Their Dynamics", 1st Canadian Discrete and Algorithmic Mathematics Conference, CanaDAM 2007, Banff, Canada, May 28-31, 2007.

- **G.-W. Weber,** "Vítejte v Praze!" – "Welcome to Prague!" - Scientific Exchange and Friendship in the Golden City of Prague, Report about Joint EUROPT-OMS Conference - 2nd Conference on Optimization Methods & Software and 6th EUROPT Workshop on Advances in Continuous Optimization, July 4-7, 2007, Prague, Czech Republic, OR News 31, 60-62, 2007.
- **G.-W. Weber, A. Tezel, Ö. Uğur, B. Akteke-Öztürk, S. Z. Alparslan-Gök, S. Özögür, P. Taylan**, "Optimization, Dynamics and Prediction of Gene-Environment Networks –Elements of Finance and Development Included", EUROPT-OMS Conference, Prague, Czech Republic, July 4-7, 2007.
- **G.-W. Weber, P. Taylan, S. Z. Alparslan Gök, B. Akteke Öztürk, S. Özöğür, Ö. Uğur, A. Tezel**, "A New Mathematical Approach in Environmental Protection: Gene- Environment Networks and Their Dynamics", EURO WG CBBM Workshop, Prague, July 8, 2007.
- **S.Özöğür, Z. Hussain, J. Shawe-Taylor,** "Model Selection via Test Margin", EURO XXII European Conference on Operational Research, Prague, July, 2007.
- **A. Gökmen, İ. Gökmen, H. Önder, G.-W. Weber**, Sustainable Living in Balaban Valley, Invited Talk, EURO-ORD Workshop "Workshop on OR for Developing Countries Young Researchers and PhD Symposium", Prague, Czech Republic July 7, 2007.
- **F. Summers, S. T. Elias-Özkan, G.-W. Weber**, Kerkenes Team: A Short Presentation and Demonstration on the Kerkenes Eco-Center Project Activities, EURO-ORD Workshop "Workshop on OR for Developing Countries Young Researchers and PhD Symposium", Prague, Czech Republic July 7, 2007.
- **P. Taylan, G.-W. Weber**, "Regression in Financial Mathematics by Additive Models and Continuous Optimization", EURO XXII 2007, Prague, Czech Republic, July 8-11, 2007.
- **Ö. Uğur, G.-W. Weber**, "A Mathematical Tutorial: Dynamics and Prediction in Gene-Environment and Financial Networks with the Help of Optimization", Tutorial, EURO XXII 2007, Prague, Czech Republic, July 8-11, 2007.
- **B. Akteke-Öztürk, G.-W. Weber**, "Data Mining for Quality Improvement Data with Nonsmooth Optimization vs. PAM and k-Means", EURO XXII 2007, Prague, Czech Republic, July 8-11, 2007.
- **G.-W. Weber, P. Taylan, S. Z. Alparslan-Gök, B. Akteke-Öztürk, S. Özöğür, A. Tezel, S. W. Pickl**, "Dynamics, Stability and Control in Environmental and Biological Dynamics", EURO XXII 2007, Prague, Czech Republic, July 8-11, 2007.
- **S. Z. Alparslan, S. Tijs, B. Karasözen, G.-W. Weber, S. Miquel**, "Cooperation under Interval Uncertainty", EURO XXII 2007, Prague, Czech Republic, July 8-11, 2007.
- **Z. Volkovich, Z. Barzily, B. Akteke-Öztürk, G.-W. Weber**, "Cluster Stability Using Minimal Spanning Trees", EURO XXII 2007, Prague, Czech Republic, July 8-11, 2007.
- **G.-W. Weber, A. Rubinov**, EUROPT Fellow 2006: One of the Architects in "OR Creates Bridges", EURO XXII 2007, Prague, Czech Republic, July 8-11, 2007.
- **P. Taylan, G.-W. Weber, N.-N. Urgan, S.W. Pickl**, "Approximation of stochastic differential equations by additive models using splines and conic programming", Invited Paper, CASYS'07, Eighth International Conference on Computing Anticipatory Systems, Liege, Belgium, August 6-11, 2007.
- **G.-W. Weber, P. Taylan**, "Regression in Financial Mathematics by Additive Models and Continuous Optimization", Invited Lecture, The 2nd Summer School "Achievements and Applications of Contemporary Informatics, Mathematics and Physics", Kiev, August 8-20, 2007.
- **B. Akteke-Öztürk, G.-W. Weber**, "Data Mining for Quality Improvement Data with Nonsmooth Optimization vs. PAM and k-Means", Invited Lecture, The 2nd Summer School "Achievements and Applications of Contemporary Informatics, Mathematics and Physics", Kiev, August 8-20, 2007.
- **G. Köksal, S. Kayalıgil, G.-W. Weber**, Data Mining in Quality Improvement, Invited Lecture, The 2nd Summer School "Achievements and Applications of Contemporary Informatics, Mathematics and Physics", Kiev, August 8-20, 2007.
- **F. Summers, S. T. Elias-Özkan, G.-W. Weber**, Kerkenes Team: a Short Presentation and Demonstration on the Kerkenes Eco-Center Project Activities, Invited Lecture, The 2nd Summer School "Achievements and Applications of Contemporary Informatics, Mathematics and

Physics", Kiev, August 8-20, 2007.

- **G.-W. Weber, S. Z. Alparslan-Gök, B. Akteke-Öztürk, S. Özöğür, P. Taylan, A. Tezel, Ö. Uğur**, Inverse Problems in Gene-Environment Networks, 6th ISAAC Congress, METU, Ankara, August 13-18, 2007.
- **G.-W. Weber, B. Akteke-Öztürk, P. Taylan, S. Özöğür Akyüz, S. Z. Alparslan-Gök**, "Optimization and Dynamics of Gene-Environment Networks", Operations Research 2007, Saarbrücken, September 5-7, 2007.
- **S. Z. Alparslan Gök, S. Tijs, B. Karasozen, G.-W. Weber, S. Miquel**, Cooperation Under Interval Uncertainty l, 22 European Conference on Operational Research, EURO Prag, 8-11 July 2007.
- **U. Kaplan, M. Türkay, L. Biegler, B. Karasözen**, "Modeling and Optimization of Metabolic Networks using Hybrid Systems Approach", 22 European Conference on Operational Research, EURO, Prag, 8-11 July, 2007.
- **B. Karasözen**, "Max-min Separability: Incremental Approach and Application to Supervised Data Classification", 22 European Conference on Operational Research, EURO Prag, 8-11 July, 2007.
- **B. Karasözen**, "Selection of Steady States in Planar Darcy Convection", ICIAM(Industrial Congress Industrial and Applied Mathematics), Zurich 16-20 July, 2007.
- **B. Karasözen**, Symplectic and multi-symplectic Lobatto methods for the "good" Boussinesq equation, ISAAC,13-18 August, METU-Ankara, 2007.
- **C.C. Küçüközmen,** Risk Management in Emerging Markets & Hedge Funds, Financial Stability Institute, BIS, Seminar on Risk Management, Beatenberg, Switzerland, May 2007.
- **M. Mazıbaş, C.C. Küçüközmen**, Forecasting the Change and Direction of Change in ISE Sector Indices: An Artificial Neural Network Application, Paper presented at the 3rd International Conference on Business, Management and Economics, Organized by Yaşar University, Çeşme, İzmir, 13-17 June 2007.
- **C.C. Küçüközmen, H. D. Oğuz**, Emerging Markets' Stock Market Volatility and Impact of News: Is it Really Observable?, Paper presented at the 3rd International Conference on Business, Management and Economics, Organized by Yaşar University, Çeşme, İzmir, 13-17 June 2007.

Yurtiçi Tebliğ	Yurtiçi Sunum
14	**16**

YURTİÇİ TEBLİĞLER

- **O. Yayla, S. Akleylek**, "PKI-Lite: A PKI System with Limited Resources", Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 59-62, Ankara, 13-14 Aralık 2007.
- **H. Özadam, F. Özbudak , Z. Saygı**, "Secret Sharing Schemes and Linear Codes", Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 101-106, Ankara, 13-14 Aralık 2007.
- **E. Akkemik, O. Kara, A. Kurşunlu**, "On Meier-Stafellbach's Fast Correlation Attack". Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 107-113, Ankara, 13-14 Aralık 2007.
- **M. Sönmez Turan, Ö. Özuğur, O. Kurt,** "Hash Function Designs Based on Stream Ciphers", Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 114-118, Ankara, 13-14 Aralık 2007.
- **A. Doğanaksoy, O. Özen, F. Sulak, K. Varıcı, E. Yüce**, "Cryptanalysis of the Dedicated Hash Functions", Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 119-126, Ankara, 13-14 Aralık 2007.
- **O. Özen, K. Varıcı,** "On the Security of the Encryption Mode of Tiger Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 127-133, Ankara, 13-14 Aralık 2007.

- **S. Akleylek, M. D. Yücel**, "Comparing Substitution Boxes of the Third Generation GSM and Advanced Encryption Standard Ciphers", Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 157-162, Ankara, 13-14 Aralık 2007.
- **O. Yayla,** "DSA Sisteminin Çalıştırılması ve Test Edilmesi", Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 290-297, Ankara, 13-14 Aralık 2007.
- **H. Özadam, O. Yayla,** "On Algebraic Attacks Using Groebner Basis", Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 312-318, Ankara, 13-14 Aralık 2007.
- **M. Cenk, F. Özbudak**, "Rings of Low Multiplicative Complexity and Fast Multiplication in Finite Fields F_2N" Bilgi Güvenliği ve Kriptoloji Konferansı, ISC'07, Bildiriler Kitabı 319-322, Ankara, 13-14 Aralık 2007.
- **E. Akyıldız, S. Akleylek,** "Kriptolojideki Gelişmeler", TMMOB Sanayi Kongresi 2007, Bildiriler Kitabı 173-178, Ankara, 14-15 Aralık 2007.
- **L. Emmungil, S. Akleylek**, Learning Content Management System: Atutor, 10th Internet Conference in Turkey, Turkey, November 8-10 2007.
- **B. Akteke-Öztürk, G.-W. Weber, S. Kayalıgil**, Kalite iyileştirmede veri kümeleme: Döküm endüstrisinde bir uygulama, in the proceedings of Yöneylem Araştırması ve Endüstri Mühendisliği 27. Ulusal Kongresi (YA/EM 2007), 1207-1212, Izmir, Turkey, July 2-4, 2007.
- **G.-W. Weber, P. Taylan, S. Özöğür, B. Akteke-Öztürk,** Statistical learning and optimization methods in data mining, in: Recent Advances in Statistics, eds.: H.Ö. Ayhan and I. Batmaz, Turkish Statistical Institute Press, Ankara, at the occasion of "Graduate Summer School on New Advances in Statistics", 181-195, August 2007

YURTİÇİ SUNUMLAR

- **A. Doğanaksoy, Ç. Çalık, F. Sulak, M. Sönmez Turan**, "Rassal Gezinti Testi", IGS06 İstatistik Gunleri Sempozyumu, Antalya, 2006.
- **B. Akteke-Öztürk, G.-W. Weber, S. Kayalıgil**, Kalite İyileştirmede Veri Kümeleme: Döküm Endüstrisinde bir Uygulama, Yöneylem Araştırması ve Endüstri Mühendisliği" Yöneylem Araştırması ve Endüstri Mühendisliği 27. Ulusal Kongresi (27th Annual Conference of the Turkish OR Society), YA/EM 2007, Izmir, Turkey, July 2-4, 2007.
- **A. Gökmen, İ. Gökmen, G.-W. Weber, D. Dinçel**, Güneşköy 2007, Video Conference on Complex Societal Problems, METU, Ankara, December 11, 2007.
- **S. Özöğür, G.-W. Weber**, Data Mining: Classification - The Example of Support Vector Machines, Invited Lecture, Graduate Summer School on New Advances in Statistics, METU, August 11-24, 2007.
- **P. Taylan, G.-W. Weber**, "Data Mining: Regression - The Example of Spline Regression and MARS, Graduate Summer School on New Advances in Statistics", Invited Lecture, METU, August 11-24, 2007.
- **A. İşcanoğlu, G.-W. Weber, P. Taylan**, Predicting Default Probabilities with Generalized Additive Models for Emerging Markets, Invited Lecture, Graduate Summer School on New Advances in Statistics, METU, August 11-24, 2007.
- **B. Akteke-Öztürk, G.-W. Weber**, Data Mining: Clustering - The Use of Optimization Theory, Graduate Summer School on New Advances in Statistics, Invited Lecture, METU, August 11-24, 2007.
- **İ. Gökmen, A. Gökmen, H. Önder, H. Tuydes, G.-W. Weber**, Sustainable Living in Balaban Valley, Workshop on Sustainable Living at Turkish Rural Countryside, METU, Ankara, June 8, 2007.
- **A. Aydın, B. Karasözen**, Lineer Olmayan İkili Schrödinger Denklemi için Yarı-Açık Simplektik ve Çoklu Simplektik Altı-Nokta Yontemleri, Erzurum Atatürk Universitesi, Ulusal Matematik Sempozyumu, 3-6 Eylül 2007.
- **A. İşcanoğlu, G.-W. Weber, P. Taylan**, Predicting Default Probabilities with Generalized Additive Models for Emerging Markets, Invited Lecture, Graduate Summer School on New

Advances in Statistics, METU, August 11-24, 2007.

- **M. Taştan, Ö. Çelik, G.-W. Weber, B. Karasözen, F. Korkusuz**, "Mathematical Modeling of Proximal Femur Geometry and Bone Mineral Density", Joint Diseases and Related Surgery 17, 3, 128-136, 2007.
- **G.-W. Weber, P. Taylan, S. Özöğür, B. Akteke-Öztürk**, "Statistical Learning and Optimization Methods in Data Mining, in: Recent Advances in Statistics", eds.: H.Ö. Ayhan and I. Batmaz, Turkish Statistical Institute Press, Ankara, at the occasion of "Graduate Summer School on New Advances in Statistics", August, 181-195, 2007.
- **C.C. Küçüközmen**, Basel-II, Construction Sector and SMEs: An Assessment within the Framework of Global Competition, *İnşaat Sanayii Dergisi*, No:101, p.34-37, May/June, 2007.
- **C.C. Küçüközmen**, GAGIAD, Basel-II and SMEs, Gaziantep, 11 May 2007.
- **C.C. Küçüközmen**, Kastamonu Ticaret Borsası, Basel-II and SMEs, Kastamonu, 31 March 2007.
- **C.C. Küçüközmen**, **A. Yüksel**, Boğaziçi University, Department of Economics Seminar, Presentation of co-authored paper titled "A Macro-econometric Credit Risk Model for Stress Testing the Turkish Credit Portfolio". İstanbul, March 16,2007.

Yurtdışı Kitapta Makale	Yurtiçi Kitap
1	**1**

YURTDIŞI KİTAPTA MAKALE

- **M. Cenk, F.Özbudak**, "Isomorphism classes of ordinary elliptic curves over fields of characteristic 3", pp. 151-158, Mathematical Methods in Engineering (eds. K. Taş, J. A. T. Machado, D. Baleanu), (2007).

YURTİÇİ KİTAP

- **E. Akyıldız, S. Akleylek, C. Çimen**, "Şifrelerin Matematiği: Kriptografi", ODTÜ Geliştirme Vakfı Yayıncılık, Mayıs 2007.

UME Preprint Serisi (IAM Preprint Series)*: 18 (No: 66-84)
(www.iam.metu.edu.tr/research Preprint Series)

*Bu Preprintlerin listesi **Ek 1**'de verilmektedir.

ÇALIŞTAY/ SEMPOZYUM/ KONFERANS/ YAZOKULU

- **Bilgi Güvenliği ve Kriptoloji Konferansı**, (13-14 Aralık 2007, Ankara)
  Uygulamalı Matematik Enstitüsü, Telekomünikasyon Kurumu ve Gazi Üniversitesi tarafından Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı (**www.iscturkey.org**) düzenlenmiştir. Türkiye'den çeşitli kamu kurum ve kuruluşları, finans kuruluşları, üniversiteler, yazılım şirketleri, elektronik sertifika hizmet sağlayıcıları ve sivil toplum kuruluşları ile dünyanın çeşitli ülkelerinden 1500'ün üzerinde temsilcinin katılımı ile gerçekleştirilmiştir. Büyük ilgi gösterilen Konferansta, Bilim Kurulunda görevli değerli hakemler tarafından uygun bulunan 41 bildiri sözlü olarak ve 15 bildiri poster olarak yer almıştır. Birinci gün düzenlenen panelde bankalar, kredi kartı kurumu, elektronik sertifika hizmet sağlayıcısı, çözüm geliştiriciler ve sivil toplum örgütünden temsilcilerden oluşan panelistler tarafından finans sektöründe kurumsal bilgi güvenliği ile ilgili olarak yaşanan son gelişmeler, istatistikler ve uygulamalar konusunda bilgiler verilmiştir. Finlandiya, Almanya, Avustralya ve Türkiye'den davetli konuşmacılar, mobil e-imza altyapısı ve bileşenleri, mobil e-imza konusunda ülke ve dünya uygulamaları, belge yönetiminde mobil e-imza uygulaması, kriptografi ve bilgi güvenliği alanındaki son gelişmeler ve uygulamalar hakkında bilgiler vermişlerdir. Uygulama sunumları bölümünde mobil e-imza, kriptoloji ve bilgi güvenliği alanında 5 adet başarılı uygulama örneği sunulmuştur.

- **EURO-CBBM Workshop-Workshop on OR in Computational Biology, Bioinformatics, and Medicine** (8 Temmuz 2007, Prague, Czech Republic)
  Bu çalıştay Çek Cumhuriyeti Prag'daki EURO 2007 toplantısı öncesinde Hesaplamalı Biyoloji, Biyoinformatik ve Tıp (EURO CBBM) (http://euro-cbb.ku.edu.tr/conference/homepage.htm) içindeki EURO çalısma grubu tarafından OR üzerine organize edilmiştir. Çalıştayın amacı Hesaplamalı Biyoloji, Bioinformatik ve Tıp alanında OR metodu kullanarak problem çözen insanları biraraya getirmektir. Bu çalıştaya tüm dünyadan 50 kişi katılmıştır.

- **EURO XXII 2007, 22nd European Conference on Operational Research** (Prague, 8-11 Temmuz, 2007)
  Bu çalıştayda, borsa için etkili bir forum ve güncel çalışmalar, yayınlar ve gelecek akımların görüşülmesi planlanmaktadır. 22. Avrupa Operasyonel Araştırma Konferansı (Conference on Operational Research EURO XXII) Prag Ekonomi Üniversitesi (http://euro2007.vse.cz/) ile Çek Operasyonel Araştırma Topluluğu tarafından organize edilmiştir. Türkiye delegasyonu tüm dünyadan katılanlar içinde 4. büyük gruptur. 2000 katılımcısı ile EURO XXII yapılmış olan en büyük EURO konferansıdır.

- **Workshop on Sustainable Living at Turkish Rural Countryside" (8 Haziran 2007 METU, Ankara)**
  Bu çalıştayın amacı, Türkiyenin az gelişmiş bölgelerindeki gelişimi, kadınların ve çocukların değişimi ve göç gibi konuları içermektedir. Bu yıl üçüncüsü düzenlenen çalıştay UME, ODTÜ, Balaban Vadisi Grubu, Kerkenes Ekolojik-Bölge Projesi, EUROPT, EURO Çalışma Grubu ve EURO Karmaşık Sosyal Problemler Çalışma Gruplarının katılımlarıyla gerçekleşmiştir.
  (http://www.iam.metu.edu.tr/EUROPT/Workshop%20on%20Complex%20Societal%20Problems.doc.)

ARAŞTIRMA GRUPLARI/ DOSAP PROGRAMI

AÇIK ANAHTAR ALTYAPISI (AAA) ARAŞTIRMA GRUBU

Açık Anahtar Altyapısı (AAA) konusunda bilgi birikimi elde etmek ve yeni gelişmeler sunmak amacıyla üç temel grup olarak araştırma yapılmaktadır. Yazılım geliştirme grubu; algoritma geliştirme, analiz ve kodlama çalışmaları yapmaktadır, hukuki işler ve uygulama grubu; kullanılacak olan teknolojilerin hukuka ve kanunlara uygunluğunu araştırmak ve konu ile ilgili çıkan yönetmelik ve tebliğleri takip etmek ve bunların projedeki uygulamaları ile ilgilenmektedir, altyapı ve sistem geliştirme grubu; proje içerisinde ihtiyaç duyulan altyapı ve sistem gereksinimlerini belirleyerek bu sistemlerin kurulumu ve güvenliği ile ilgilenmektedir. (www.pki.iam.metu.edu.tr)

AKAN ŞİFRE SİSTEMLERİ ÇALIŞMA GRUBU

Akan Şifre Sistemleri Çalışma Grubunun araştırma alanları akan şifre sistemlerinin test, tasarım ve analiz konularını içermektedir. Grup bu amaçla literatürde bilinen birçok akan şifre sisteminin yanısıra, ECRYPT Stream Cipher Project'e sunulan birçok algoritmanın tasarımlarını incelemekte ve analizlerini yapmaktadır. Aynı zamanda akan şifrelerin genel test yöntemleri ve tasarım kriterlerinin geliştirilmesi konularında da çalışmalar yapılmaktadır.

BOOLE FONKSİYONLARI ÇALIŞMA GRUBU

Bu grubun amacı, dengelilik, tam çığ ölçütü (strict avalanche criterion), yüksek nonlineerite, yüksek cebirsel derece, yüksek mertebede korelasyon bağışıklığı ve yüksek mertebede propagation kriteri gibi konuları çalışmaktadır. Bu fonksiyonların tasarımında bütün bu karakteristikler hesaba katılmalıdır. Örneğin bükük fonksiyonlar (Benting functions) maksimum nonlineeriteye sahiptir ve sıfırdan farklı her vektör için propagation kriteri sağlar. Fakat bu fonksiyon sınıfı dengeli ve korelasyon bağışıklı değildir. Boole fonksiyonları kriptografinin önemli bir alanı olmuştur. Shannon 1949 yılında modern kriptografinin temellerini attığında çarpım şifrelerini ifade etmek için permütasyon ve yer değiştirme olmak üzere iki temel dönüşüm kullanmıştır. Kullandığı her iki dönüşümde de Boole fonksiyonların kriptografik özellikleri sözkonusudur. Bundan sonraki süreçte kriptolojide Boole fonksiyonları S-kutuları tasarımında yaygın bir şekilde kullanılmıştır. Boole fonksiyonunun iyi olmasının ölçüsü kriptografik özellikleriyle doğru orantılıdır. (http://www.math.metu.edu.tr/bfwg)

DİNAMİK SİSTEMLER ARAŞTIRMA GRUBU

"Uygulamalı Dinamik Sistemler" araştırma grubu güncel matematiğin en faal alanlarından biri olan Dinamik Sistemler Teorisinin biyoloji, tıp, ekonomi ve finans gibi alanların problemlerine uygulamaları üzerine yoğunlaşmıştır. UME, Elektrik-Elektronik, Biyoloji, Matematik Bölümlerinden bazı öğretim üyelerinden oluşan bu grup modellerinde, fonksiyonel ve impulsive differensiyel denklemler kullanmakta ve somut problemlerin incelenmesinde çatallanma teorisi, merkez manifold teorisi gibi soyut teorilerden yararlanmaktadır. (http://www.iam.metu.edu.tr/research)

EUROPT OPTİMİZASYON ARAŞTIRMA GRUBU

Bu araştırma grubunun amacı, uluslararası işlevsel araştırma ve uygulamalı matematik çalışmalarını özellikle avrupa birliğindeki araştırmacılarla birlikte uluslararası düzeyde canlı tutmaktır. EUROPT Optimizasyon Araştırma Gurubu olarak popüler dergilerin özel sayılarına yayınlar hazırlanmış, birçok çalıştay düzenlenmiş, her düzeyde çeşitli bilimsel aktiviteler gerçekleştirilmiştir. Bunların dışında iki yeni EURO çalışma grubu ile çalışmalar devam etmekte ve 2003 yılından itibaren Uygulamalı Matematik Enstitüsü, EUROPT ve EURO Sürekli Optimizasyon çalışma grubuna ev sahipliği yapmaktadır. (http://www.iam.metu.edu.tr/EUROPT/)

FİNANSAL RİSK ARAŞTIRMA GRUBU

Finansal Risk Araştırma Grubu Türk finans sektöründe uygulama ve teoride karşılaşılan problemleri çözmek üzere 2003 yılında enstitümüz bünyesinde kurulmuş bir araştırma grubudur. Bu araştırma gurubu üniversite ile finans kurumlarının risk birimi çalışanlarını bir araya getirerek söz konusu problemlerin anlaşılmasını ve çözüm önerileri üretilmesini sağlamak amacını gütmektedir.
(http://www.iam.metu.edu.tr/research/groups/riskman.html)

HESAPLAMALI BİYOLOJİ VE TIP ARAŞTIRMA GRUBU

Bu araştırma grubunda yer alan temel konular, gen ekspresyon motiflerinin modellenmesi ve tahmini, hesaplamalı insan metabolizması, beyin araştırmaları, kalp araştırmaları, populasyon dinamiği, gen dinamiği, gen değişimleri (populasyonların sınıflandırılması), sürdürebilir gelişme, ve dünya ısısının kontrolüdür. Bu grup ODTÜ'de Biyoinformatik/Hesaplamalı Biyoloji üzerine **Bilim ve Teknolojileri YUUP Grubu** ile ortak çalışmaktadır. **YUUP araştırma grupları**'nda, biyoteknoloji, tıp ve biyoinformatik gibi araştırma konuları ile ilgili birçok temsilcisi bulunmaktadır.
(http://www.iam.metu.edu.tr/research/groups/compbio/index.html)

HİBRİD SİSTEMLER ARAŞTIRMA GRUBU

"Development of Modeling and Optimization Tools for Hybrid Systems" NSF-TÜBİTAK INT ve "Modeling Multistationary Processes by Using Hybrid System Formulation: A study with priority on functional genomics" TÜBİTAK kariyer projesi çerçevesinde çalışmalar sürdürülmektedir.
(http://www.iam.metu.edu.tr/research/groups/hybrg/index.html)

KODLAMA TEORİSİ ARAŞTIRMA GRUBU

Ana uygulamasının iletilerde oluşan hataların saptanması/düzeltilmesi olan hata düzeltici kodlar, özellikle otantikasyon kodlarıyla kriptografiye ve bilginin lineer olarak işlendigi başka alanlara da uygulanabilmektedirler. İyi parametrelere sahip kodların çok noktalı cebirsel eğrilerden ve varyetelerden elde edildiği bilinmektedir. Bu araştırma grubunun ilgi alanları: iyi parametrelere sahip hata düzeltici kod inşaası, sonlu cisimler üzerindeki cebirsel eğriler ve varyeteler, çok noktalı eğriler inşaası ve bu eğrilerden kodlar üretilmesi ve kodlama teorisinin kriptografiye uygulamaları sayılabilir. Ayrıca hata düzeltme kodları kullanılarak doğrulama kodlarının oluşturulması da amaçlanmaktadır.

OPTİMİZASYON TEORİSİ ARAŞTIRMA GRUBU

Bu araştırma grubu global, yarı-sonsuz değişkenli, türevsiz ve düzgün olmayan optimizasyon konularında çalışmalar yapmaktadır. (http://www.iam.metu.edu.tr/EUROPT)

TERS PROBLEMLER ARAŞTIRMA GRUBU

Grubun 2007 yılı çalışmaları, diğer grupların çalışmalarına ve projelerine destek şeklinde, ortaklaşa yürütülmüştür. (http://www.iam.metu.edu.tr/research)

DOSAP PROGRAMI

- **Pakize Taylan** (Dicle Üniversitesi, Matematik Bölümü), Finansal Piyasalarda Matematiksel Optimizasyon Tekniklerinin Kullanımı (1 Ekim 2005- 1 Eylül 2007)
- **Nedim Dikmen** (Giresun Üniversitesi, Ekonometri Bölümü), Faiz haddinin modellenmesi: Makro Finans yaklaşımı (1 Eylül 2006- 1 Eylül 2007).

YÜRÜTÜCÜLÜĞÜ YAPILAN PROJELER

Projenin Adı: Kriptografi Konusunda Araştırma, Geliştirme; Algoritma Tasarımı, Analizi ve Uygulanması (BAP-07-05-DPT.2004K120700 DPT)
Yürütücüsü: Ersan Akyıldız
Araştırmacıları: Rüyal Ergül, Ali Doğanaksoy, Melek Yücel, Ferruh Özbudak, Muhiddin Uğuz, Emrah Çakçak, A. Devin Sezer, Zülfükar Saygı, Meltem Sönmez
Süresi: 1.1.2004-31.12.2007
Bütçesi: 2.650.980- YTL

Projenin Adı: Açık Anahtar Altyapı Konusunda Araştırma, Geliştirme Ve Uygulamalar (TÜBİTAK Kamu Projesi)
Yürütücüsü*: Rüyal Ergül
Araştırmacıları: Ali Doğanaksoy, Ferruh Özbudak, Muhiddin Uğuz, Emrah Çakçak, Mustafa Alkan, K. Sacit Sarıkaya, Sezen Yeşil, Özgür Öztürk, Onur Gençer, Meltem Sönmez, Oğuz Yayla, Deniz Toz
Süresi: 1.7.2006-1.7.2008
Bütçesi: 450.000- YTL

Projenin Adı: Modeling Multistationary Processes by Using Hybrid System Formulation: A study with priority on functional genomics (TÜBİTAK 1001 Projesi)
Yürütücüsü: Hakan Öktem
Araştırmacıları: Didem Akçay, Özgür Hakanoğlu
Süresi: Haziran 2005 –Haziran 2010
Bütçesi: 162.400- YTL

Projenin Adı: Nükleer Füzyon Reaktör Problemlerinin Sınır Elemanları ve Sonlu Elamanlar Yöntemleri ile Çözümü (TÜBİTAK 1001 Projesi)
Yürütücüsü: M. Tezer
Araştırmacıları: Ali İhsan Neslitürk, Selçuk Han Aydın, Sevin Gümgüm
Süresi: 1 Kasım 2005 – 1 Kasım 2007
Bütçesi: 41.100- YTL

Projenin Adı: Sabit Faiz Oranlı Mortgage Kontratlarının Enflasyonist Ekonomilerde Fiyatlandırılması: Türkiye Örneği (TÜBİTAK 1001 Projesi)
Yürütücüsü: Işıl Erol
Araştırmacıları: Kasırga Yıldırak, Ömür Uğur
Süresi: 15 Ekim 2007 – 15 Ekim 2009
Bütçesi: 59.500- YTL

Projenin Adı: Özet Fonksiyon Algoritması Geliştirme Projesi (TÜBİTAK 1001 Projesi)
Yürütücüsü: A. Doğanaksoy
Araştırmacıları: Fatih Sulak, Celebi Kocair, Onur Özen, Kerem Varıcı
Süresi: 1 Ekim 2007 -1 Ekim 2008
Bütçesi: 61.150- YTL

Projenin Adı: Sürekli Optimizasyon Yöntemleri ve Uygulamaları (TÜBİTAK Bütünleşik Doktora Programı projesi)
Yürütücüsü: Bülent Karasözen
Araştırmacıları: Gerhard W. Weber, Tanıl Ergenç, Yusuf Uludağ
Süresi: 2005-...

***** Bu projenin yürütücülüğünü 30 Kasım 2007 tarihinden itibaren Ersan Akyıldız yapmaktadır.

Projenin Adı: Özgün Eliptik Eğri Tasarlanması ve Eliptik Eğri Tabanlı Algoritma Uygulamalarının Geliştirilmesi (ASELSAN)
Yürütücüsü: Ersan Akyıldız, Rüyal Ergül
Süresi: 1.10.2006-30.3.2008
Bütçesi: 200.000- YTL

Projenin Adı: Blok Tipi Algoritmaların İstatistiksel ve Yapısal Test Yazılımlarının Geliştirilmesi (ASELSAN)
Yürütücüsü: Ali Doğanaksoy
Süresi: 1.12.2006-30.11.2007
Bütçesi: 100.000- YTL

Projenin Adı: Doğrulama Kodlarının Üretilme Metodlarının İncelenmesi, Geliştirilmesi ve Uygulanması (BAP-2006-07-05-02)
Yürütücüsü: Ferruh Özbudak
Araştırmacıları: Murat Cenk, Zülfükar Saygı, Emrah Çakçak.
Süresi: 1.1.2006-31.12.2007
Bütçesi: 8.000- YTL

Projenin Adı: Biyolojik Veri Madenciliğinin ve Sınıflandırılmasının İstatistiksel Öğrenmesi, Sürekli Optimizasyon, Makina Öğrenmesi ve Semi(yarı)-Sonsuz Programlama Kullanılarak Geliştirilmesi (BAP-2007-07-05-02)
Yürütücüsü: Gerhard W. Weber
Araştırmacıları: Zümrüt B. Ögel, Bülent Karasözen, Volkan Atalay, John Shawe Taylor, Pakize Taylan, Ömür Uğur, Süreyya Özöğür
Süresi: 1 Ocak 2007 – 31 Aralık 2008
Bütçesi: 5.500- YTL

Projenin Adı: Enflasyona Endeksli Finansal Ürünlerin Fiyatlandırılması (BAP-2007-07-05-05)
Yürütücüsü: Hayri Körezlioğlu
Araştırmacıları: Ş. Kasırga Yıldırak, Nedim Dikmen, Sühan Altay, Ayşegül İşcanoğlu, Zehra Ekşi, İ.Ethem Güney, Nilüfer Çalışkan
Süresi: 1 Ocak 2007-31 Aralık 2007
Bütçesi: 3.000- YTL

Projenin Adı: Kartezyen Hesaplama Ağı Üreticisi Geliştirilmesi (BAP-2007-07-05-03)
Yürütücüsü: Mehmet Haluk Aksel
Araştırmacıları: Bülent Karasözen
Süresi: 1 Ocak 2007-31 Aralık 2008
Bütçesi: 6.000- YTL

Projenin Adı: Gayrimenkul Yatırımlarında Enflasyon Riskine Karşı Korunma: Markov Rejim Değişim Modeli Uygulaması (BAP-2007-07-05-04)
Yürütücüsü: Işıl Erol
Araştırmacıları: Kasırga Yıldırak
Süresi: 1 Ocak 2007-31 Aralık 2007
Bütçesi: 7.312- YTL

Projenin Adı: Dynamic Importance Sampling and NATREX (BAP-2007-07-05-06)
Yürütücüsü: Ali Devin Sezer
Araştırmacıları: -
Süresi: 1 Şubat 2007-1 Haziran 2007
Bütçesi: 500- YTL

Projenin Adı: Optimal Investment with Random Investment Times (BAP-2007-07-05-07)
Yürütücüsü: Ali Devin Sezer
Araştırmacıları: -
Süresi: 15 Şubat 2007-15 Ağustos 2007
Bütçesi: 2.000- YTL

Projenin Adı: Meteoroloji ve oşinografideki veri asimilasyonunda arka plan hataların farklı yöntemlerle hesaplanması ve karşılaştırılması (BAP-2007-07-05-00-01)
Yürütücüsü: Bülent Karasözen
Araştırmacıları: Murat Akman
Süresi: 1 Ocak 2007-31 Aralık 2007
Bütçesi: 1.500- YTL

Projenin Adı: Development of Modeling and Optimization Tools for Hybrid Systems (NSF-TÜBİTAK INT projesi)
Yürütücüsü: B. Karasözen
Araştırmacıları: L. Biegler (Koç Üniversitesi ve Carnegie Mellon Üniversitesi Kimya Müh. Bl.), H. Öktem, M. Türkay ve U. Yılmaz (Koç Üniversitesi, Endüstri Müh. Bl.)
Süresi: 2005-2007

ENSTİTÜ BAĞLANTILI ÖĞRETİM ÜYELERİNİN ARAŞTIRMACI OLARAK KATILDIKLARI PROJELER

Projenin Adı: Kalite İyileştirmede Veri Madenciliği Kullanımı ve Geliştirilmesi (TÜBİTAK Araştırma projesi)
Yürütücüsü: G. Köksal (Endüstri Mühendisliği)
Araştırmacıları: B. Karasözen, G. W. Weber
Süresi: 2005-2008

Projenin Adı: Dışsal değişkenlerin yarattığı belirsizlik ortamında en uygun para politikasının belirlenmesi (TÜBİTAK Hızlı Destek SOBAG Projesi)
Yürütücüsü: Ümit Özlale (Bilkent Üniversitesi Ekonomi Bölümü)
Araştırmacıları: A. Devin Sezer
Süresi: 1 Kasım 2007 – 1 Kasım 2008
Bütçesi: 27.500- YTL

Projenin Adı: Meteoroloji/Oşinografi Mükemmeliyet Ağı (MOMA) pilot projesi: Uydu ve yer gözlem, veri asimilasyonu, öngörü, erken uyarı sistemleri ve kullanıcı hizmetleri geliştirilmesi (TÜBİTAK Kamu projesi)
Yürütücüsü: E. Özsoy (Deniz Bilimleri Endüstri)
Araştırmacıları: B. Karasözen, Ö. Uğur, H. Öktem
Süresi: 2005-2007

Projenin Adı: Composable Derivative Contracts (ComDeCo Projesi)
Yürütücüsü: Ralf Korn (Univ. of Kaiserslautern), Arnd Poetzsch-Heffter
Araştırmacıları: Stefanie Müller, Ulrich Nögel, Markus Reitz, Ömür Ugur
Süresi: 2005 - 2007

Projenin Adı: Balaban Valley Project Sürekli Optimizasyon Yöntemleri ve Uygulamaları
Yürütücüsü: A. Gökmen
Araştırmacıları: S. Kayalıgil, G. W. Weber, İ. Gökmen, M. Ecevit, A. Sürmeli, T. Bali, Y. Ecevit, H. Gökmen, D. J. DeTombe
Süresi: 2004-...

ÖĞRETİM ÜYESİ YETİŞTİRME PROGRAMI (ÖYP) PROJELERİ

Danışmanı: Hayri Körezlioğlu/Ömür Uğur
Öğrencinin Adı: Ayşegül İşcanoğlu
Üniversitesi: Selçuk Üniversitesi, KONYA
Bütçesi: 2.357

Danışmanı: Marat Akhmet/Ömür Uğur
Öğrencinin Adı: Derya Altıntan
Üniversitesi: Selçuk Üniversitesi, KONYA
Bütçesi: 2.620

Danışmanı: -
Öğrencinin Adı: Nüket Erbil
Üniversitesi: Fırat Üniversitesi, ELAZIĞ
Bütçesi: 2.162

Danışmanı: Ersan Akyıldız
Öğrencinin Adı: Barış Bülent Kırlar
Üniversitesi: Süleyman Demirel Üniversitesi, ISPARTA
Bütçesi: 3.758

Danışmanı: G. Wilhelm Weber
Öğrencinin Adı: S. Zeynep Alparslan
Üniversitesi: Süleyman Demirel Üniversitesi, ISPARTA
Bütçesi: 5.083

Danışmanı: Melek D. Yücel
Öğrencinin Adı: Sedat Akleylek
Üniversitesi: Ondokuz Mayıs Üniversitesi, SAMSUN
Bütçesi: 3.198

Danışmanı: Ersan Akyıldız
Öğrencinin Adı: Turgut Hanoymak
Üniversitesi: Yüzüncü Yıl Üniversitesi, VAN
Bütçesi: 2.180

Danışmanı: Melek D. Yücel
Öğrencinin Adı: Rita İsmailova
Üniversitesi: Kırgız Türkiye Manas Üniversitesi, KIRGIZİSTAN
Bütçesi: 2.891

Danışmanı: Melek D. Yücel
Öğrencinin Adı: Nurbek Ulu Baryk
Üniversitesi: Kırgız Milli Üniversitesi, KIRGIZİSTAN
Bütçesi: 2.723

DİĞER FAALİYETLER

KISA SÜRELİ KURSLAR/SEMİNERLER

- **Regina Burachik** (South Australia University), "Lectures on Advanced Optimization", 1 Agustos - 15 Ekim 2007.
- **Yalçın Kaya** (South Australia University), "Inexact Restoration Method for Optimal Control", 1 Agustos - 15 Ekim 2007.
- **Michael Hinze** (University of Hamburg), "Lectures on pde constrained optimization" 15-19 Ekim 2007.
- **Asuman Özdağlar** (Massachusetts Institute of Technology), "Subgradient methods: theory and applications" 24-29 Aralık 2007.
- **Stef Tijs** (University of Tilburg), "Lectures on Cooperative Game Theory", 17-31 Haziran 2007.

ENSTİTÜMÜZÜ KISA SÜRELİ ZİYARET EDENLER

- **Stef Tijs- Radica Branzei**, Center and Department of Econometrics and Operations Research, Tilburg University, The Netherlands, July 17-31, 2007.
- **Regina Burachik**, Department of Mathematics, University of Southern Australia, Adelaide, July 20 – October 13, 2007.
- **Yalcın Kaya**, Department of Mathematics, University of Southern Australia, Adelaide, July 20 – October 13, 2007.
- **Michael Hinze**, Department of Mathematics, University of Hamburg, Germany, October 15-19, 2007.
- **Asuman Özdağlar**, Electrical Engineering and Computer Science Department, Massachusetts Institute of Technology, USA, December, 24 - 29, 2007.
- **Sebastien Blais,** Departement de sciences economiques, Universite de Montreal, Canada, October 21, 2007.
- **Michael Hinze,** Department of Mathematics, University of Hamburg) October 16, 2007.
- **Hendrik W. Lenstra,** September 23–26, 2007.
- **Erhan Bayraktar,** Dept. of Mathematics, University of Michigan, USA, July 30–August 4, 2007.
- **Martin Rainer** (Value & Risk AG, Frankfurt am Main) March 19–23, May 29–30, July 17–18, 2007.
- **Klaus Schmidt,** University of Erlangen, Germany, March 6, 2007.
- **İsmail Yücel**, Center for Atmospheric Sciences, Hampton University, May 29, 2007.
- **Serpil Kocabıyık,** Memorial University, Department of Mathematics and Statistics, Newfoundland and Labrador, Canada, September 1- December 31, 2007.
- **Serdar Boztaş** RMIT University, Melbourne, Australia, December 10-14, 2007.
- **Sebastien Blais,** University of Montreal, Canada, presently at Bilkent University, November 21, 2007.
- **Can Akkoç,** University of South Alabama, Dept. of Comparative Medicine, Alabama, February-September 2007.

ENSTİTÜ ÜYELERİNİN KISA SÜRELİ YURT DIŞI ZİYARETLERİ

- **S. Zeynep Alparslan Gök**, Tilburg Üniversitesi, Hollanda, 29 Ocak – 14 Mart 2007.
- **Ömür Uğur**, Kaiserslautern Üniversitesi ve Fraunhofer Enstitüsü, Almanya,1 Şubat - 21 Eylül 2007.
- **Süreyya Özöğür**, University College London, İngiltere, 1 Ocak – 16 Şubat 2007, 1-14 Temmuz 2007.
- **B. Karasözen**, Technical University of Darmstadt, University of Augsburg, Technical University of Karlsruhe, Almanya, 5 Haziran – 5 Agustos 2007.
- **B. Karasözen,** Carnegie Mellon University, University of Houston, Amerika, 20 Agustos-8 Eylül 2007.

ENSTİTÜ DESTEKLİ KONFERANS KATILIMLARI

- **F. Rüyal Ergül,** İstanbul 2007 ICT, Conference on Research and Development, İstanbul, 29-31 Ocak 2007.
- **Sedat Akleylek,** Web Uygulamalarında Güvenlik ve Kablosuz Yerel Ağlarda Güvenlik, Kütahya, 30 Ocak 2007.
- **Meltem Sönmez Turan,** SASC07-The State of Art of Stream Ciphers, Almanya, 31 Ocak -1 Şubat 2007.
- **Zülfükar Saygı,** International Workshop on Coding and Crptography (WCC 2007), Fransa, 16-20 Nisan 2007.
- **Elif Saygı,** Third International Workshop on Boolean Functions: Cryptography and Applications. Fransa, 2-3 Mayıs 2007.
- **Ersan Akyıldız,** International Conference on Security of Information and Networks (SIN 2007), Kıbrıs, 8-10 Mayıs 2007.
- **Oğuz Yayla,** International Conference on Security of Information and Networks (SIN 2007), Kıbrıs, 8-10 Mayıs 2007.
- **Ahmet I. Seven,** Perspectives in Auslander-Reiten Theory, Norveç, 10-12 Mayıs 2007.
- **F. Rüyal Ergül,** Industry-Academia Patternship and Pathways: IAPP, Bürüksel, 16 Mayıs 2007.
- **Ersan Akyıldız,** EUROCRYPT 2007, İspanya, 20-24 Mayıs 2007.
- **Nedim Dikmen,** 8. Ulusal Ekonometri ve İstatistik Sempozyumu, Malatya, 24-25 Mayıs 2007.
- **Marat Akhmet,** Fift International Conference on Dynamical Systems and Applications, Amerika, 28 Mayıs-5 Haziran 2007.
- **Ersan Akyıldız,** Projective Geometry and Commutative Algebra in Applications, İtalya, 15-16 Haziran 2007.
- **Emrah Çakçak,** Summer School in Göttingen NATO Advanced Study Institute on Higher-Dimensional Geometry over Finite Fields, Almanya, 25 Haziran-6 Temmuz 2007.
- **Gerhard Wilhelm Weber,** 6th EUROPT Workshop on Advances in Continuous Optimization, Prag Çek Cumhuriyeti, 4-7 Temmuz 2007.
- **Gerhard Wilhelm Weber,** EURO XXII 2007 European Conference on Operational Research, Prag Çek Cumhuriyeti, 8-11 Temmuz 2007.
- **Ali Devin Sezer,** EURO XXII 2007 European Conference on Operational Research, Prag Çek Cumhuriyeti, 8-11 Temmuz 2007.
- **Pakize Taylan,** EURO XXII 2007 European Conference on Operational Research, Prag Çek Cumhuriyeti, 8-11 Temmuz 2007.
- **Süreyya Özöğür,** EURO XXII 2007 European Conference on Operational Research, Prag Çek Cumhuriyeti, 8-11 Temmuz 2007.
- **Işıl Erol,** The 12th Asian Real Estate Society (AsRES) Annual Conference and the 2007 AREUEA International Conference, Çin, 07-13 Temmuz 2007.
- **Bülent Karasözen,** ICIAM 2007, Zürih, 16-20 Temmuz 2007.
- **Zaliha Yüce,** CEBİT 2007, İstanbul 2 Ekim 2007.
- **Sedat Akleylek,** 3th International Conference on Information Technologies and Telecommunication (ITTC 2007), Azerbaycan, 4-6 Ekim 2007.
- **Meltem Sönmez Turan,** Indocrypt 2007, Hindistan, 9-13 Aralık 2007.
- **Selçuk Kavut,** The 17th International Applied Algebra, Algebraic Algoriths, and Error Correcting Codes (AAECC-17), Hindistan, 16-20 Aralık 2007.
- **Ersan Akyıldız,** Asiacrypt 2007, Malezya, 2-6 Aralık 2007.
- **Ferruh Özbudak,** Arithmetic, Geometry, Crytography and Coding Theory, Fransa, 5-9 Kasım 2007.

KONFERANS/ÇALIŞTAY/YAZ OKULU/DİĞER ÜYELİKLER

- **G.-W. Weber**, Member in Scientific Committee of The International Workshop of Wavelets to Real World Problems II: IWW2007, Isparta, Turkey, June 7-9, 2007.
- **G.-W. Weber**, Member of Program Committee of A Joint EUROPT-OMS Conference, Chair of the Program Committee and Chairman of a session, Prague, Czech Republic, July 4-7, 2007.
- **G.-W. Weber**, Member of Organizing Committee of PhD Workshop in OR for Development: EURO Working Group OR for Development, Prague, Czech Republic, July 7, 2007.
- **G.-W. Weber**, Member of International Program Committee of 8th International Conference CASYS'07, on Computing Anticipatory Systems, International Conferences on Computing Anticipatory Systems in Liege, Belgium, August 6-11, 2007.
- **G.-W. Weber**, Member of Organizing and Program Committees of Video Conference on Complex Societal Problems, METU, Ankara, and University of Amsterdam, The Netherlands, December 11, 2007.
- **G.-W. Weber**, Member in Program Committee of Nonconvex Programming: Local and Global Approaches, Theory, Algorithms and Applications, Rouen, France, December 17-21, 2007.
- **G.-W. Weber**, Member of Editorial Board of Journal of Computational Technologies, 2007.
- **G.-W. Weber**, Member of Program Committee of INFORMS International 2007, Puerto Rico, July 8-11, 2007.

EKLER

EK: 1
IAM PREPRINT SERİSİ

IAM PREPRINT SERIES

No	Title - Abstract	Author	Date
66	Cluster Stability Using Minimal Spanning Trees	Z.V. Volkovich, Z. Barzily, B. Akteke-Öztürk and G.W. Weber	08.01.2007
67	On Optimization,Dynamics and Uncertainty:a Tutorial for Gene-Environment Networks	G.W.Weber, Ö.Uğur,P.Taylan,A.Tezel	15.01.2007
68	Pattern Analysis for the Prediction of Eukoryatic Pro-peptide Cleavage Sites	S.Özöğür,J.Shawe-Taylor,G.-W.Weber and Z.Begüm Ögel	21.01.2007
69	A New Mathematical Approach in Environmental and Life Sciences:Gene-Environment Networks and Their Dynamics	G.W.Weber, S.Z.Alparslan-Gök, B.Söyler	20.02.2007
70	Algebraic Properties of the Operations used in Block Cipher IDEA	H.M. Yıldırım, and E. Akyıldız	08.03.2007
71	A ptototype Compartmental Model of Blood Pressure Distribution	M. Akhmet	21.03.2007
72	On the Parameter Estimation for Generalized Partial Linear Models with B-Splines and Continuous Optimization	Pakize Taylan and G.W. Weber	10.04.2007
73	Cooperation Under Interval Uncertainty	S.Z. Alparslan-Gök,S. Miquel,S. Tijs	12.04.2007
74	Mathematical and Data Mining Contributions to Dynamics and Optimization of Gene-Environment Networks	G.W. Weber, P. Taylan, B.A. Öztürk and Ö. Uğur	08.05.2007
75	Kalite İyileştirmede Veri Kümeleme : Döküm Endüstrisinde Bir Uygulama	B.A. Öztürk, G.W. Weber and S. Kayalıgil	18.06.2007
76	Max-min separability : incremental approach and application to supervised data classfication	A.M. Bagirov, D. Webb and B. Karasözen	19.06.2007
77	Multivariate Adaptive Regression Spline and Continuous Optimization for Modern Applications in Science, Economy and Technology	P. Taylan, G.W. Weber	26.07.2007
78	Statistical Learning and Optimization Methods in Data Mining	G.W. Weber, P.Taylan, S. Özöğür, B. Akteke-Öztürk	01.07.2007
79	On Vasicek Stochastic Interest Rate Process with Stochastic Volatility	A. Bastıyalı Hayfavi	14.08.2007
80	Selection of steady states in planar Darcy convection	B. Karasözen, V.G. Tsybulin	27.09.2007
81	Cosymmetric families of steady states in 3D convection of incompressible fluid in a porous medium	V.G. Tsybulin, A.D. Nemtsev, B. Karasözen	27.09.2007
82	Environmental and Life Sciences : Gene-Environment Networks-Optimation, Games and Control-A Survey on Recent Achievements	G.W. Weber, S.Z. Alparslan-Gök, N. Dikmen	22.10.2007
83	"Staggered grids discretization in three-dimensional Darcy convection	B. Karasözen, A.D. Nemtsev, V.G. Tsybulin	23.10.2007
84	Continuous Optimization Applied in MARS for Modern Applications in Finance, Science and Technology	P. Taylan, G.W. Weber, F. Yerlikaya	26.10.2007
85	Semi-Infinite and Conic Optimization in Modern Human, Life and Financial Sciences under Uncertainty	G.W. Weber, E. Kropat, S.Z. Alparslan-Gök	6.12.2007
86	Learning with Infinitely Many Kernels via Semi-Infinite Programming	S. Özöğür-Akyüz, G.W. Weber	18.12.2007

EK: 2
UME SEMİNERLERİ

Genel Seminerler

Networks' Challenge: Where Game Theory Meets Network Optimization	**Asuman Özdağlar** Massachusetts Institute of Technology	25.12.2007
Image Regularization: The Role of Numerics	**Sibel Tarı** METU, Dept. of Computer Engineering	18.12.2007
Randomness and Pseudo-randomness in Secure Communications	**Serdar Boztaş** Rmit University, Melbourne, Australia	11.12.2007
Yazılım Büyüklük Ölçme ve İşgücü Kestirimi	**Çiğdem Gencel**	20.11.2007
Information Geometry	**Muazzez Şimşir** (TOBB University of Economy and Technology, Dept. of Mathematics)	13.11.2007
A large deviation upperbound for a buffer overflow event of a Markov modulated queuing network	**A. Devin Sezer** (UME)	06.11.2007
Numerical Simulation of free surface flows with arbitrarily moving bodies	**Serpil Kocabıyık** (Memorial University, Dept. of Mathematics and Statistics, Newfoundland and Labrador, Canada)	30.10.2007
Two Algorithms fort pense he Minimum Enclosing Ball Problem	**Emre Alper Yıldırım** (Bilkent University)	23.10.2007
Recent Trends and Challenges in pde Constrained Optimization	**Michael Hinze** (Dept. of Mathematics, University of Hamburg)	16.10.2007
A New Approach in Financial Mathematics and Science: Aproximation of Stochastic Differential Equations by Additive Models Using Splines and Conic Programming	**Gerhard-Wilhelm Weber** (UME)	09.10.2007
Inexact Restoration Method for Optimal Control	**Yalçın Kaya** (School of Mathematics and Statistics, University of South Australia)	02.10.2007
On the Pricing of American Options for Jump Diffusions	**Erhan Bayraktar** (Dept. of Mathematics, University of Michigan)	02.08.2007
Satellite Data Assimilation in Hydrometeorological Model systems	**İsmail Yücel** (Center for Atmospheric Sciences, Hampton University)	29.05.2007
Abstract and title to be announced	**Erkut Erdem** (METU, Dept. of Computer Engineering)	15.05.2007
The story of Perelman and some problems of organization of science: reflection on ethics, politics and research	**Sergei Finashin** (METU, Dept. of Mathematics)	08.05.2007
Shapiro Inequalities	**Cem Tezer** (METU, Dept. of Mathematics)	24.04.2007
Title to be Announced	**Hüseyin Şirin Hüseyin** (Atılım Üniversitesi, Dept. of Mathematics)	10.04.2007
Transcendental numbers and Riemann surfaces	**Hurşit Önsiper** (METU, Dept. of Mathematics)	03.04.2007
Financial option valuation in practice	**Martin Rainer** (Value & Risk AG, Frankfurt am Main)	20.03.2007
Two Notions of Category in Linguistics: Some (Really Naive) Algebra	**Cem Bozşahin** (METU, Dept. of Computer Engineering)	13.03.2007

Yaşam ve İnsan Bilimleri ve Ekonomi Alanında Uygulamalı Matematik Seminerleri

Interval-Valued Cooperative Games	**S. Zeynep Alparslan-Gök** (UME)	14.12.2007
Characterization of Electrical Activity of the Heart from Intravenous Catheter Measurements: Feasibility of Signal Processing and Computer Simulation Approaches	**Bülent Yılmaz** (Başkent University, Biomedical Engineering Dept.)	07.12.2007
Long-term economic growth for Turkey	**Sumru Altuğ** (Koç University, College of Administrative Sciences and Economics,)	30.11.2007
Grid-Connected Variable Speed Generator Application with Doubly-Fed Induction Machine	**Erhan Demirok** (Sabancı University, Faculty of Engineering and Natural Sciences)	23.11.2007
Linear and Support Vector Machines	**Güvenç Arslan** (Başkent Üniversitesi, İstatistik ve Bilgisayar Bilimleri Bölümü)	16.11.2007
Various Topics of Applied Mathematics Computational Statistics and Data Mining - the Examples of Clustering, Classification and Regression	**Gerhard-Wilhelm Weber** (UME)	09.11.2007
Gezgin Satici Ve Araç Rotalama Problemleri	**İmdat Kara** (Başkent Üniversitesi Müh. Fak.)	02.11.2007
A Study on Joint Distribution of Fuzzy Dependent Risks	**Fatih Tank** (Kırıkkale Universitesi, Dept. of Statistics)	26.10.2007
Türk Makam Mûsıkîsinde İcraya Dayalı Nazariyat Modeli Geliştirilmesi Üzerine	**Can Akkoç** (University of South Alabama, Dept. of Comparative Medicine, Mobile, Alabama)	05.10.2007
Computational Statistics and Data Mining - the Examples of Clustering, Classification and Classification	**Gerhard-Wilhelm Weber** (UME)	28.09.2007
Integration of Topological Measures for Eliminating Non-Specific Interactions in Protein Interaction Networks	**Tolga Can** (METU, Dept. of Computer Engineering)	21.09.2007
Population modeling for a captive squirrel monkey colony	**Can C. Akkoç** (University of South Alabama, Dept. of Comparative Medicine, , Mobile, Alabama)	22.06.2007
Sustainable Living in Balaban Valley	**Ali Gökmen, İnci Gökmen** (METU, Dept. of Chemistry)	08.06.2007
Challenges schools face due to internal migration flows in Turkey	**Hanife Akar**	08.06.2007
Secure Multiparty Overall Mean Computation via Oblivious Polynomial Evaluation	**Mert Özarar** (METU, Dept. of Computer Engineering,)	01.06.2007
The Inverse Problem of Magnetoencepkalography: Sourse Localization and The Shape of Ball	**Neslihan Ozmen, Fatma Yerlikaya, Doga Gürsoy** (UME)	25.05.2007
Iterative Methods for Discrete Tomography Implementation & Comparison Kaczmarz's Method and Conjugate Gradient Least Squares Method	**Nurgül Gökgöz, Serdar Tanil, Ahmet Onur**	25.05.2007
Kerkenes Team: Demonstration of Solar Cooking and a Short Presentation on the Kerkenes Eco-Center Project Activities	**Kerkenes Team c/o Instructor Francoise Summers** (METU, Dept. of Architecture)	22.05.2007
Analysis of time-varying biomedical signals	**Elif Derya Übeyli** (TOBB Economics and Technology University, Dept, of Electrical and Electronics Engineering)	18.05.2007

New Approaches Mathematical Modeling of Proximal Femur Geometry and Bone Mineral Density	**Gerhard-Wilhelm Weber** joint work with Mesut Taştan, Özgür Çelik, Feza Korkusuz and Bülent Karasözen	11.05.2007
New Biotechnology and the Ethical Issues	**Ufuk Gündüz** (METU, Dept. of Biology)	04.05.2007
Tikhonov Regularization for Learning as an Inverse Problem	**Başak Akteke-Öztürk, Pakize Taylan, Süreyya Özöğür** (UME)	27.04.2007
The Analysis of Patterns and Foundations of Computational Statistics	**Süreyya Özöğür** (UME)	20.04.2007
Cooperation Under Interval Uncertainty	**S.Zeynep Alparslan-Gök** (UME)	13.04.2007
Energy Consumption Patterns and Sustainable Energy Sources	**İnci Gökmen** (METU, Department of Chmistry)	06.04.2007
On modified Crank-Nicholson difference schemes for stochastic parabolic equation	**Allaberen Ashyralyev** (Fatih University, Dept. of Mathematics)	30.03.2007
Inverse Problems ---in the Sectors of Life Sciences, Technology, Economy and Society	**Gerhard Wilhelm Weber** (UME)	23.03.2007
Identification of the new immunogenic proteins of Bordetella Pertussis by Immunoproteomics	**Emrah Altındiş** (METU, Depat. of Biotechnology)	16.03.2007
Virtual biomechanical analysis and finite element modeling of medical implants	**Feza Korkusuz** (METU, Medical Center, Department of Physical Education and Sports and IAM)	09.03.2007
Dynamics of the World Terror and the War in Iraq	**Güngör Gündüz** (METU, Dept. of Chemical Engineering,)	02.03.2007
A New Mathematical Approach in Environmental Protection: Gene-Environment Networks and Their Dynamics	**Gerhard Willhelm Weber** (UME)	23.02.2007
The analysis of auditory evoked brain potentials in recurve archery	**Hayri Ertan** (METU, Dept. of Physical Education and Sports)	16.02.2007
From Randomness to Regularity	**Caglar Tuncay** (METU, Dept. of Physics)	09.01.2007

Dinamik Sistemler Grup Seminerleri

Mathematical Bases of Neural Network Theory	**Enes Yılmaz** (UME)	29.11.2007
Modeling of Hopfield Neural Networks	**Enes Yılmaz** (UME)	22.11.2007
Approximating DDE by Piecewise Linear Systems with Delay	**Mustafa Kahraman** (UME)	15.11.2007
How we could find a periodic solution of the oscillatory model with a relay forcing?	**Cemil Büyükadalı** (METU, Dept. of Mathematics)	08.11.2007
The period doubling bifurcation technique in M. Feigin's paper	**Marat Akhmet** (METU, Deparment of Mathematics,)	08.11.2007
Lyapunov-Razumikhin method for differential equations with piecewise constant argument	**Duygu Arugaslan** (Deparment of Mathematics, METU)	01.11.2007

Özel Seminerler

Derivation of a stock option price under Vasicek interest rates **(Seminar on Finance)**	**Zehra Ekşi** (UME)	26.12.2007
The Inference for Weakly Identified State-Space Models: A Bayesian Analysis of Affine Term Structure Model	**Sebastien Blais** (Departement de sciences economiques, Universite de Montreal, Canada)	21.11.2007
Current Problems in Pricing of Structured Products and Derivatives on Interest, FX, Commodities and Credits	**Martin Rainer** (Value & Risk AG, Frankfurt am Main)	30.05.2007
Electronic Resources in Mathematics at METU Library	**Şemsa Güzeldere** (Middle East Technical University, Library)	01.05.2007
Merkezdeki Banka: Merkez Bankaciliginin Politik Ekonomisi ve TC Merkez Bankasi	**Caner BAKIR** (Koc Universitesi)	26.04.2007

EK: 3
EĞİTİM VE ÖĞRENCİ İSTATİSTİKLERİ

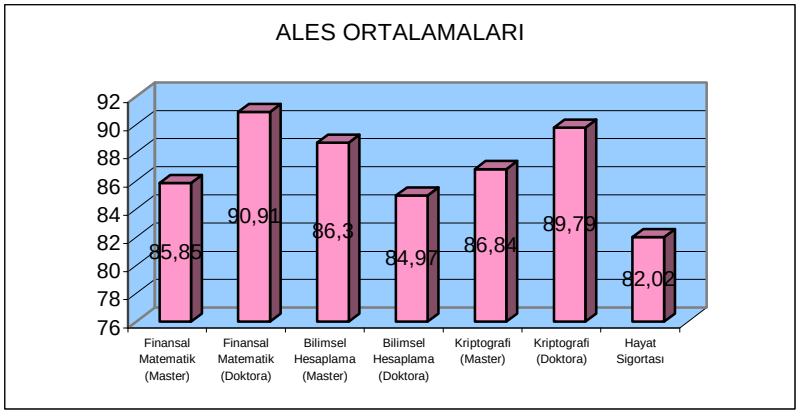
*** Veriler http://oidb.metu.edu.tr adresinden temin edilmiştir.**

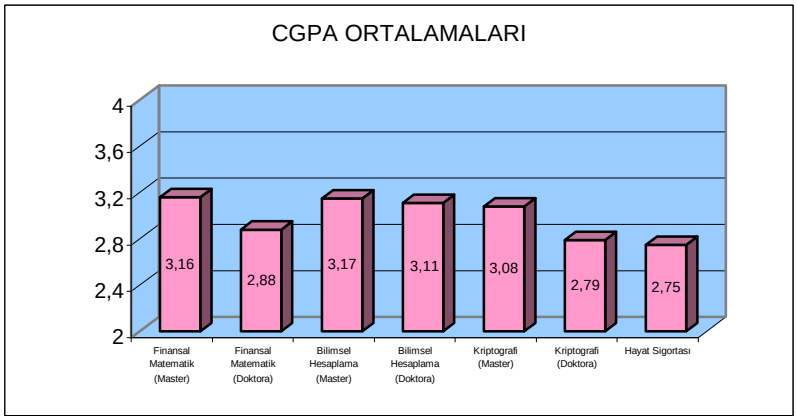
BAŞVURULAR

	2007-2008		
	BAŞVURU	**KABUL**	**KAYIT**
Bilimsel Hesaplama	24	14	12
Finansal Matematik	62	35	23
Hayat Sigortası	10	6	0
Kriptografi	40	26	23
Toplam	**136**	**81**	**58**

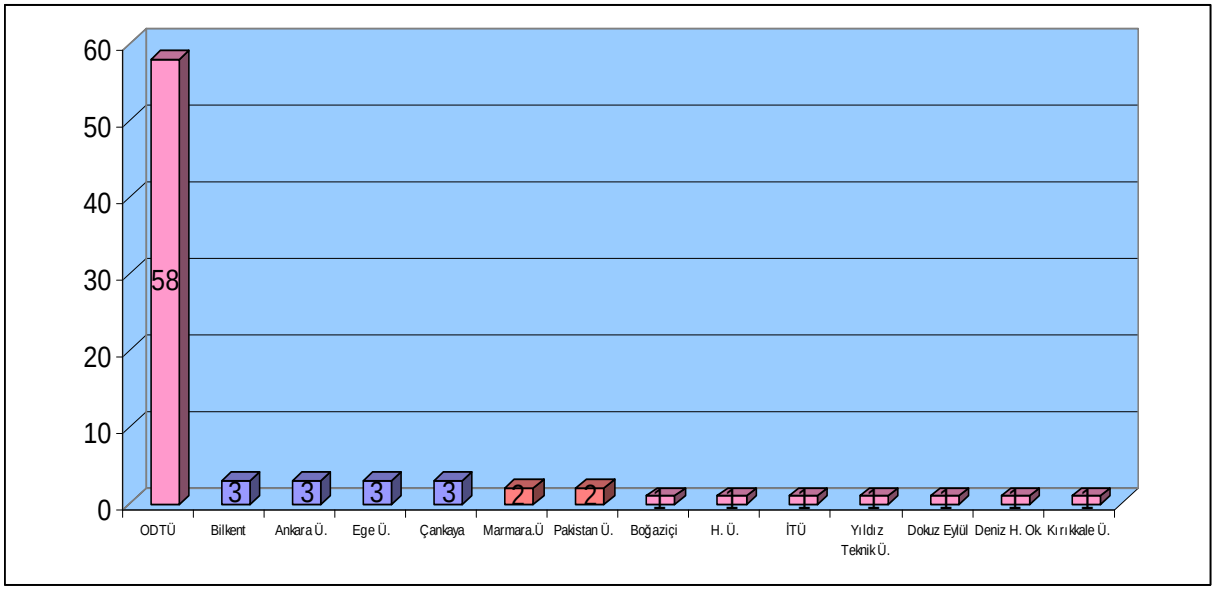
UME ÖĞRENCİLERİNİN LES VE CGPA ORTALAMALARI

2007-2008 KABUL EDİLEN ÖĞRENCİLER





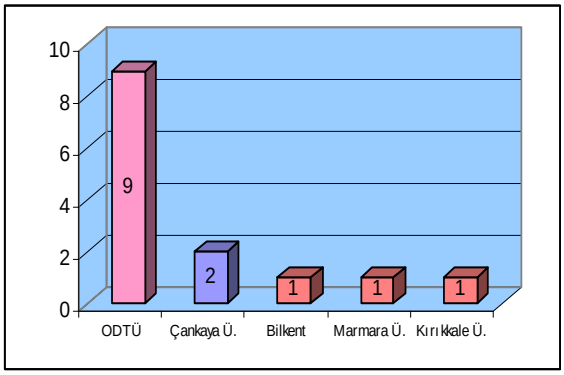
UME'YE KABUL EDİLEN ÖĞRENCİLERİN MEZUN OLDUKLARI ÜNİVERSİTELERE GÖRE DAĞILIMI



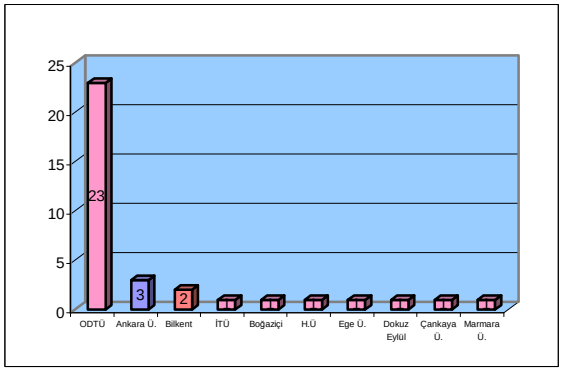
UME'YE KABUL EDİLEN ÖĞRENCİLERİN LİSANS DERECESİNİ ALDIKLARI ÜNİVERSİTELER

2007-2008

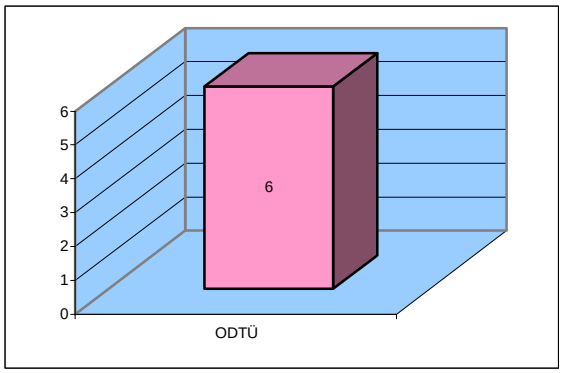
BİLİMSEL HESAPLAMA



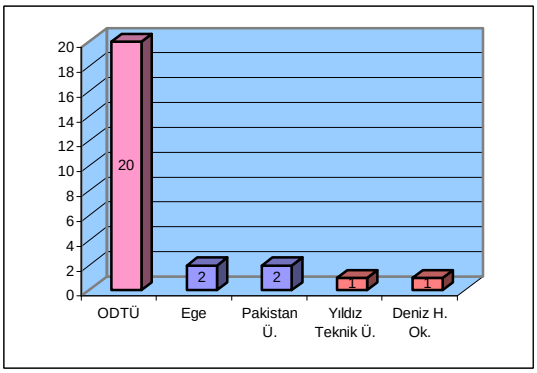
FİNANSAL MATEMATİK



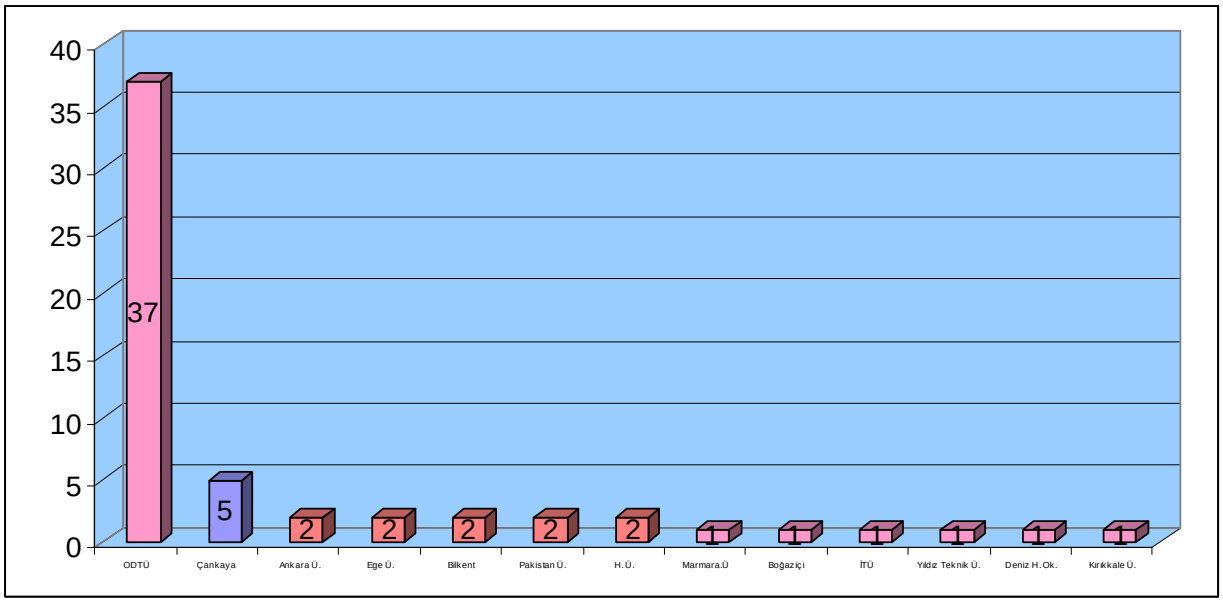
HAYAT SİGORTASI



KRİPTOGRAFİ



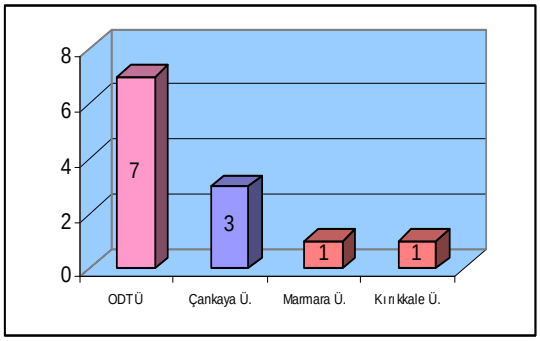
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN MEZUN OLDUKLARI ÜNİVERSİTELERE GÖRE DAĞILIMI



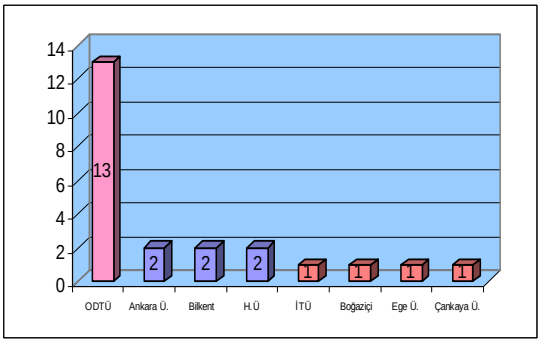
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN LİSANS DERECESİNİ ALDIKLARI ÜNİVERSİTELER

2007-2008

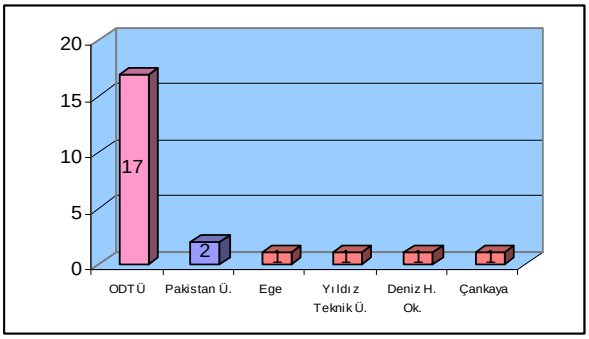
BİLİMSEL HESAPLAMA



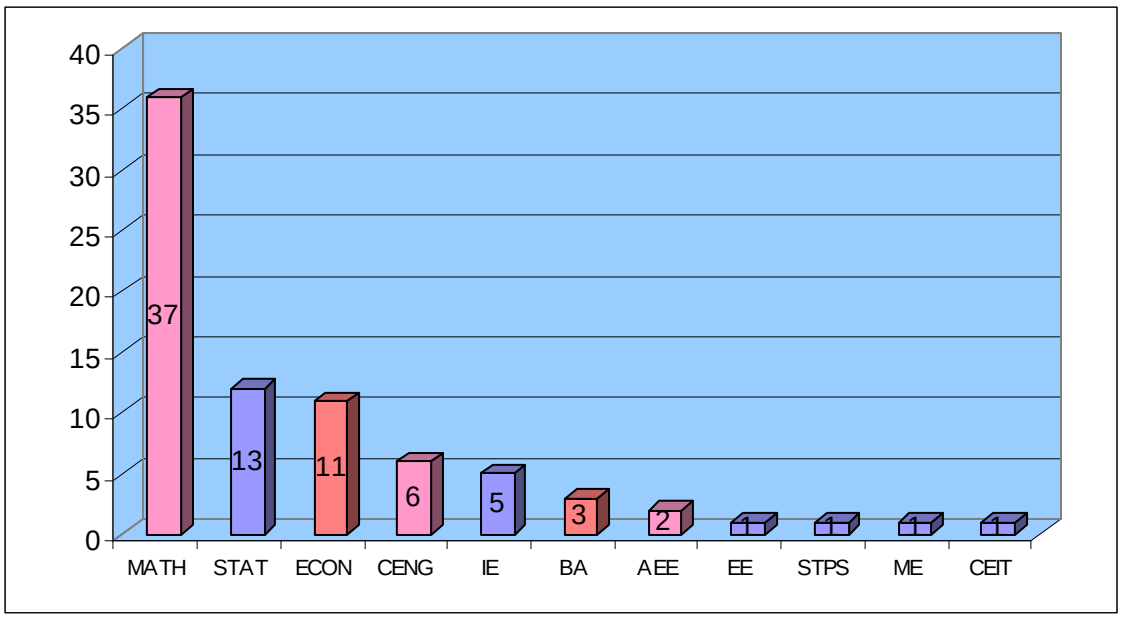
FİNANSAL MATEMATİK



KRİPTOGRAFİ



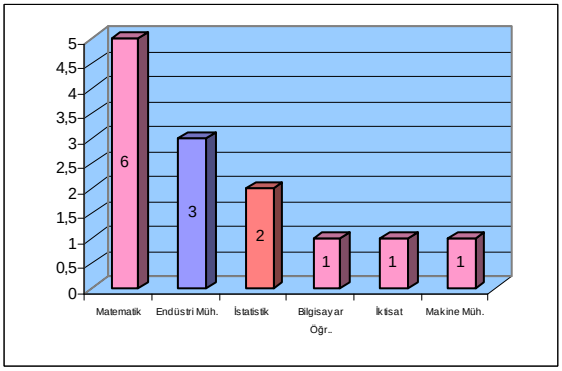
UME'YE KABUL EDİLEN ÖĞRENCİLERİN MEZUN OLDUKLARI BÖLÜMLERE GÖRE DAĞILIMI



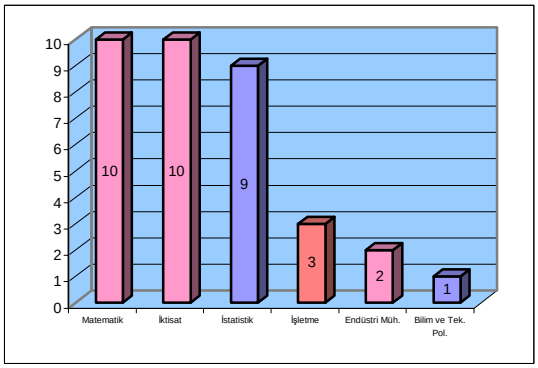
UME'YE KABUL EDİLEN ÖĞRENCİLERİN LİSANS DERECELERİNİ ALDIKLARI BÖLÜMLER

2007-2008

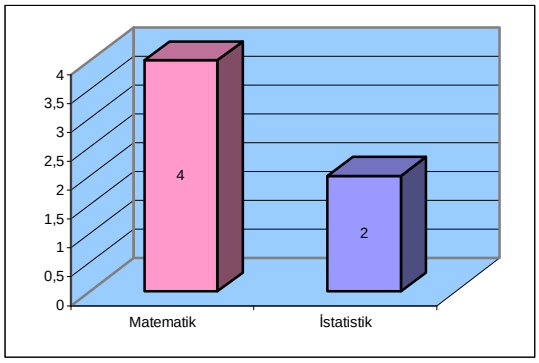
BİLİMSEL HESAPLAMA



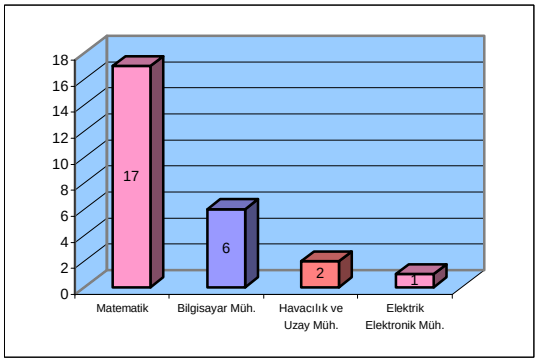
FİNANSAL MATEMATİK



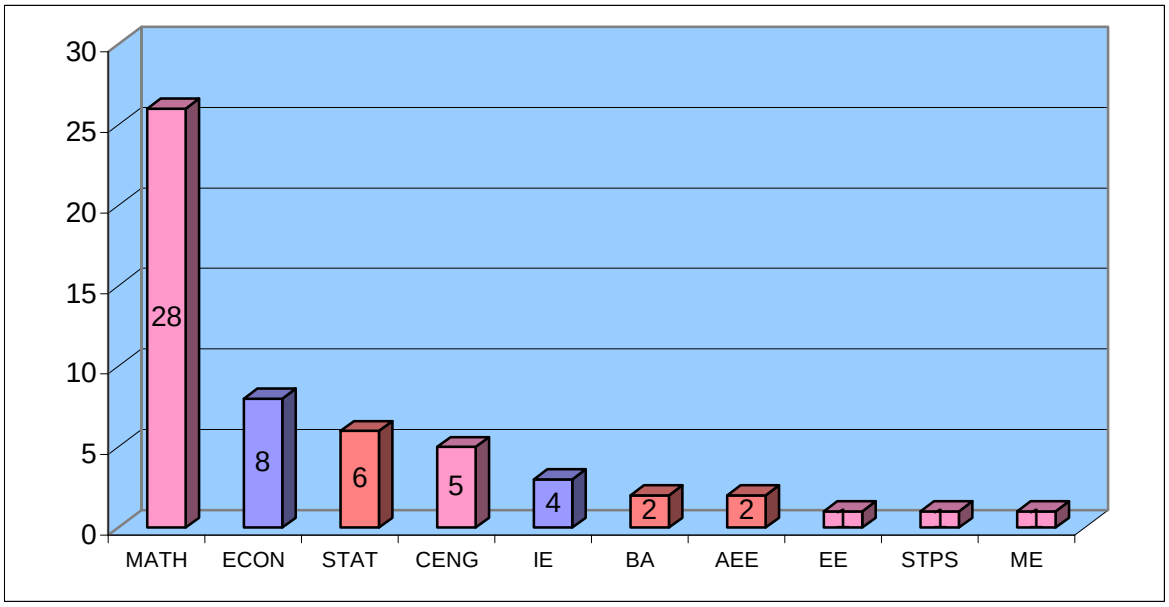
HAYAT SİGORTASI



KRİPTOGRAFİ



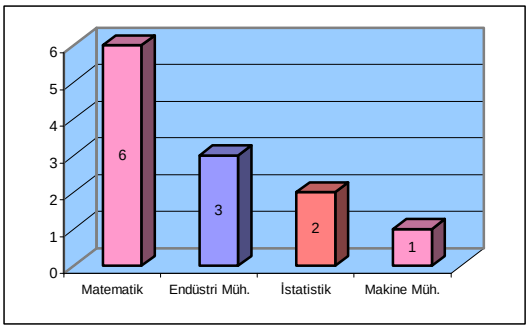
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN MEZUN OLDUKLARI BÖLÜMLERE GÖRE DAĞILIMI



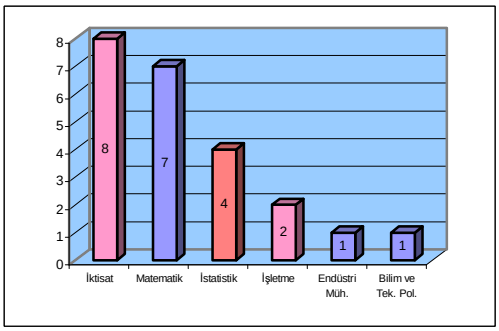
UME'YE KAYIT YAPTIRAN ÖĞRENCİLERİN LİSANS DERECELERİNİ ALDIKLARI BÖLÜMLER

2007-2008

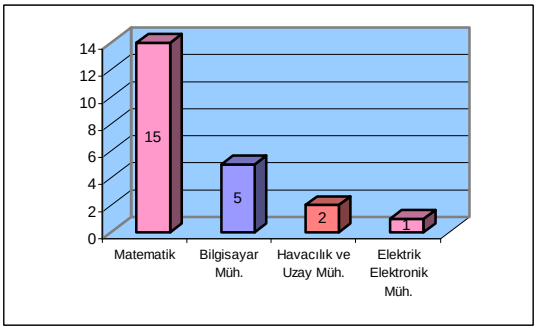
BİLİMSEL HESAPLAMA



FİNANSAL MATEMATİK

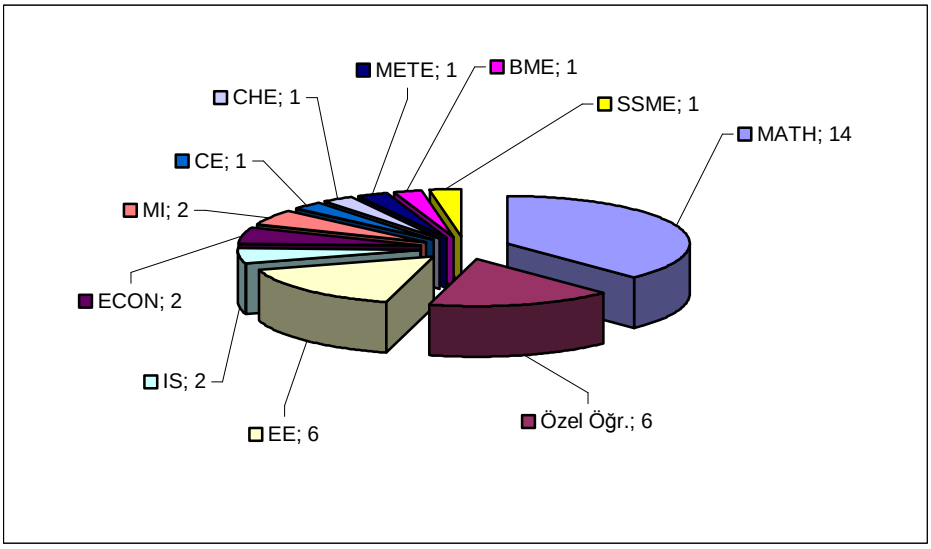


KRİPTOGRAFİ



UME DERSLERİNİ ALAN UME DIŞI ÖĞRENCİLERİN BÖLÜMLERE GÖRE DAĞILIMI

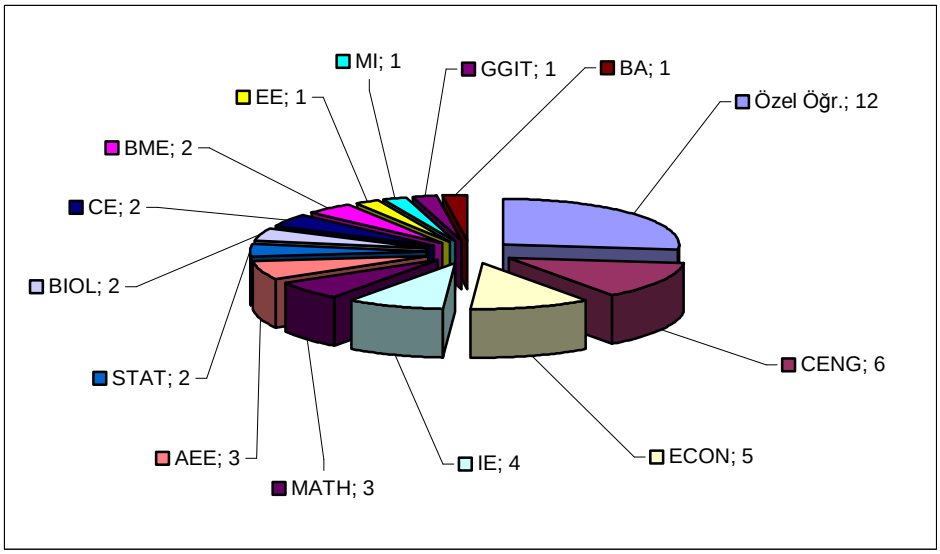
2006-2007 II.Dönem



Toplam Öğrenci Sayısı = 241

UME Dışı Öğrenci Sayısı = 37 (15%)

2007-2008 I.Dönem

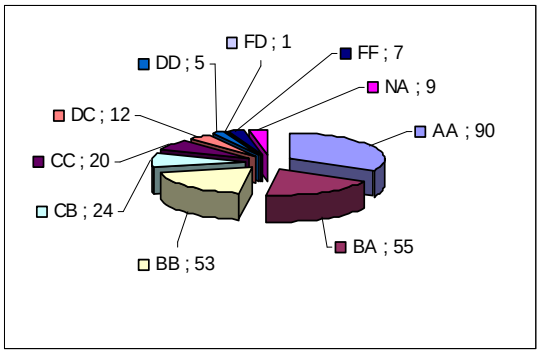


Toplam Öğrenci Sayısı = 280

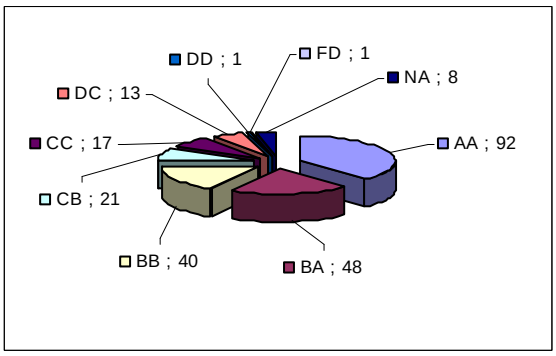
UME Dışı Öğrenci Sayısı = 45 (16%)

DÖNEMSEL VERİLEN TOPLAM NOT SAYISI

2006-2007 I. Dönem



2006-2007 II. Dönem



EK: 4
2007 YILINDA MEZUN OLAN ÖĞRENCİLER

Kriptografi Programı

Zülfikar Saygı	"Constructions of Authentication Codes" (Doktora Tezi)	**Ferruh Özbudak**
Orhan Çetinkaya	"Verifiability and Receipt-Freeness in Cryptographic Voting Systems" (Doktora Tezi)	**Ali Doğanaksoy**
Onur Özen	"On the Security of The Tiger Hash Function" (Y. Lisans Tezi)	**Ali Doğanaksoy**
İlksen Acunalp*	"Related Key Attack and Slide Atack" (Bitirme Projesi)	**Ali Doğanaksoy**
Ceyda Mangır	"Time Memory Tread of Attac Using Rainbow Tables" (Bitirme Projesi)	**Ali Doğanaksoy**
Ömer Sever*	"Optimal Extension Field: Software and Hardware Implementation" (Bitirme Projesi)	**Emrah Çakçak**
Bülent Yılmaz	"Time- Memory Trade-Off Using Distinguished Points" (Bitirme Projesi)	**Ali Doğanaksoy**
Zaliha Yüce*	"Smartcard &Cryptography" (Bitirme Projesi)	**Ersan Akyıldız**
Arda Züber	"A Study On Time-Memory Trade-Off Using Hellman Method" (Bitirme Projesi)	**Ali Doğanaksoy**
Sedat Akleylek*	"On the Avalanche Properties Of Misty1, Kasumi and Kasumi With Rijndael S-Box" (Y. Lisans Tezi)	**Melek D. Yücel**

Bilimsel Hesaplama Programı

Mustafa Kahraman	"Modelling Functional Dynamical Systems by Piecewise Linear Systems with Delay" (Y.Lisans Tezi)	**Hakan Öktem**
Ahmet Melih Selçuk	"Inference of Piecewise Linear Systems with an Improved Method Employing Jump Detection" (Y. Lisans Tezi)	**Hakan Öktem**
Muhammad Alkın	"Text Mining: A Burgeoning Quality Improvment Tool From Applied Mathematics" (Y. Lisans Tezi)	**G. Wilhelm Weber**

Finansal Matematik Programı

Havva Özlem Dursun*	"Jump Detection With Power And Bipower Variation Processes" (Y. Lisans Tezi)	**Azize Hayfavi**
İnci Esen	"How Does The Stock Market Volatility Change After Inception Of Futures Trading? The Case Of The Ise National 30 Stock Index Futures Market" (Y. Lisans Tezi)	**Seza Danışoğlu**
Orçun Kaya*	"Static hedging strategies for barrier options and their robustness to model risk'' (Y. Lisans Tezi)	**Azize Hayfavi**
Sühan Altay	"On Forward Interest Rate Models: Via Random Fields and Markov Jump Processes" (Y. Lisans Tezi)	**Hayri Körezlioğlu**
Ayhan Yüksel	"Modelling Credit Risk With Stochastic Volatility, Jumps and Stochastic Interest Rates" (Y. Lisans Tezi)	**Ersan Akyıldız**

***** Enstitümüzde doktoraya devam eden öğrenciler

EK: 5
YENİ AÇILAN DERSLER

2006–2007 Bahar Dönemi

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Numerical Methods for Financial Models**
Course Code:	**IAM 611**
Credit:	(3-0) 3
Instructor's Name:	Dr. Ali Devin Sezer (devin@metu.edu.tr)
Prerequisites:	Some understanding of the following subjects will be necessary: probability theory, optimal control, martingale theory, stochastic integration.
Content:	Three of the main tasks in financial data analysis are: Estimation of probabilistic models from real data, i.e., statistics, Computation of probabilities (e.g., value at risk, probability of ruin) and expactations (e.g, derivative pricing) in the estimated models. Optimization (e.g., american option pricing, portfolio optimization). This course looks at these problems and the mathematical and computational methods to approach them.
Aims/ Learning Outcomes:	The course will emphapsize both theory and practice. The aim is for the student to build a unified and intuitive understanding of the above problems and have at least some practical understanding and experience about how to approach them. Regular homeworks and programming problems will be assigned. Programming assignments will be coded in MATLAB. There will be an inclass midterm and a take home final exam. The homeworks will constitute 40% of the grade, the midterm and the final 30% each.
Suggested Textbooks:	Textbooks We will use parts of the following books. The instructor will provide lecture notes and other neccessary course material. Paul Glasserman, *Monte Carlo Methods in Financial Engineering*. John C Hull, *Options, Futures and Other derivatives*. Lapeyre, Sulem and Talay, *Understanding Numerical Analysis for Financial Models*. Cont and Tankov, *Financial Modelling with Jump Processes*. Lipster and Shiryaev, *Statistics of Random Processes*. Dupuis and Kushner, *Numerical Methods for Stochastic Control Problems in Continuous Time*. Additional reference books Fleming and Richel, *Deterministic and Stochastic Optimal Control*. Evans, *Partial Differential Equations*. Soner and Fleming, *Controlled Markov Processes and Viscosity Solutions*. Karatzas and Shreve, *Brownian Motion and Stochastic Calculus*. Karatzas and Shreve, *Methods of Mathematical Finance*. Protter, *Stochastic Integration and Differential Equations*.
Outline:	In all the problems we will study, the course will always begin from the simplest of models and gradually look at models of increasing complexity. Review Throughout the course we will review briefly the following topics as we need them: Continuous stochastic processes (Stochastic integration, SDEs, Martingale theory, Girsanov's theorem and the related PDE theory), Optimal Control, Discontinous stochastic proccesses, Fundamental concepts, ideas and models in Finance (replication based pricing, hedging, complete/incomplete markets, several important interest rate and market models). Statistics Value at risk, model building approach, [JCH] John C. Hull, *Options, Futures and Other Derivatives*, Section 18.3. Estimating volatilities and correlations [JCH], Chapter 19 Statistics for Diffusion Processes, Lapeyre, Sulem and Talay, *Understanding Numerical Analysis for Financial Models*, preprint, Chapter 10. Inverse problems and Model calibration, Rama Cont and Peter Tankov, *Financial Modeling with Jump processes*, Chapter 13. Calibration of an HJM model. Time permitting, we would like to also study Bayesian methods for model estimation. Computation and Optimization. For this part of the course we will mainly follow the preprint version of the book by Lapeyre, Sulem and Talay and Glasserman's Monte Carlo Methods in Financial Engineering: Option Pricing and PDEs. Finite Difference Methods for option prices. Finite Difference Methods for stochastic optimal control problems. Tree Methods for option prices. Monte Carlo and Importance Sampling for option pricing and risk estimation. Monte Carlo methods for pricing american options .

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Elliptic Curve Cryptography**
Course Code:	**IAM 711**
Credit:	(3-0)3
Instructor's Name:	Prof. Dr. Ersan Akyıldız (ersan@metu.edu.tr)
Prerequisites:	Consent of the Instructor
Content:	Algorithms to compute the number of points of an Elliptic Curve, Divisors , Pairings, The crypto system based on pairings, isomorphism attacks to elliptic curve discrete logarithm problem (ECDLP) and the other attacks.
Aims:	The aim of this course is to study the isomorphism attacks to ECDLP and as well as Schoof and Schoof-Atkin -Elkin's algorithms to compute the number of points of an Elliptic Curve. After introducing the basic facts about divisors on curves, we shall introduce The Weil Pairing and The Tate-Lichtenbaum pairing on elliptic curves. MOV attack, attack to Anomalous curves and other attacks of this nature will be discussed. Cryptosystem based on pairings , Supersingular Elliptic Curves and their use in cryptography and some other applications of Elliptic Curves in Cryptography such as primality and factorization tests will also be discussed.
Learning Outcomes:	L.C.Washington, Elliptic Curves, Number Theory and Cryprography, Chapman&Hall/CRC
Suggested Textbooks:	D. Hankerson, A. Menezes,S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, QA 76.9.A25, H38, 2004. Henri Cohen and Gerhard Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman &Hall/CRC, QA 567.2. E 44H36, 2005 I.Blake,G.Seroussi and N. Smart, Elliptic Curves in Cryptography, London Math.Soc. Lec.Note Series. No.256, 1999, QA 76.9 .A.25.B57 Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Applications of Finite Fields to Cryptography**
Course Code:	**IAM 712**
Credit:	(3-0)3
Instructor's Name:	Y. Doç. Dr. Emrah Çakçak (cakcak@metu.edu.tr)
Prerequisites:	Consent of department
Content:	The primary focus of this course is to give structure theory of Finite Fields and the related mathematical tools that are needed in Cryptography: Polynomials over finite fields, factorization of Polynomials over finite fields, Exponential Sums, Gröbner Basis Algorithms and Their Applications to Cryptography will be discussed.
Learning Outcomes:	▪ Overview of finite fields (1 weeks) o Characterization of finite fields o Field extensions o Traces, Norms and Bases o Roots of Unity ▪ Polynomials over finite fields (2 weeks) o Order of Polynomials and Primitive Polynomials o Irreducible Polynomials o Construction of Irreducible Polynomials o Linearized Polynomials o Binomials and Trinomials ▪ Factorization of Polynomials (2 weeks) o Factorization over small finite fields o Factorization over large finite fields o Calculation of roots of polynomials ▪ Exponential Sums (2 weeks) o Characters o Gaussian sums o Some Special Exponential Sums ▪ Applications in Cryptography (signatures, encryption, authentication) (4 weeks) o Hidden Fields Equations (HFE) o Isomorphism of Polynomials (IP) o HFE - Variations and Attacks Gröbner Basis Algorithms and Their Applications to Cryptography (3 weeks)
Learning Outcomes:	Advanced level of finite fields and its cryptographic applications.
Suggested Textbooks:	R. Lindl and H. Niederreither, Introduction to Finite Fields and Their Applications.

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Actuarial Risk Theory**
Course Code:	**IAM 746**
Credit:	(3-0)3
Instructor's Name:	Y. Doç. Dr. Fatih Tank (fatihtank@gmail.com)
Prerequisites:	Consent of the Instructor.
Content:	Basic concepts of probability in connection with Risk Theory; introduction to risk processes (claim number process, claim amount process, total claim number process, total claim amount process, inter-occurance process); convolution and mixed type distributions; risk models (individual and collective risk models); numerical methods (simple methods for discrete distributions, Edgeworth approximation, Esscher approximation, normal power approximation); premium calculation principles; Credibility Theory; retentions and reinsurance; Ruin Theory; ordering of risks.
Aims :	The aim of this course is to give the fundamental concepts of actuarial risk theory and to teach the role of statistics on actuarial concepts and the methods optimal decision and management in insurance.
Outline:	Week 1-2. Basic concepts of probability in sense of risk theory. Week 3 Introduction to risk processes (claim number process, claim amount process, total claim number process, total claim amount process, inter-occurance process) Week 4 Convolution and mixed type distributions Week 5-6 Risk models (individual and collective risk models) Week 7-8 Numerical methods (simple methods for discrete distributions, Edgeworth approximation, Esscher approximation, normal power approximation) Week 9-10 Premium calculation principles Week 11 Credibility Theory Week 12 Retentions and reinsurance Week 13 Ruin theory Week 14 Ordering of risks
Learning Outcomes:	The course will provide basic knowledge for advanced actuarial techniques. After taking the course, the students will have obtained a certain amount of knowledge on Actuarial Risk Theory which they may use in their future research activities.
Suggested Textbooks:	Course notes H. Bühlmann, Mathematical Methods in Risk Theory, Springer-Verlag (1970) W.R. Heilmann, Fundamentals of Risk Theory, (1988) R. Kaas, M.J. Goovaerts, J. Dhaene, M. Denuit, Modern Actuarial Risk Theory, Kluwer Academic Publisher, (2001)

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Quantitative Finance I**
Course Code:	**IAM 747**
Credit:	(3-0)3
Instructor's Name:	Assoc. Prof. Dr. Kasırga Yıldırak (kasirga@metu.edu.tr)
Prerequisites:	IAM 544
Content:	Pricing financial instruments, algorithms and programming. Econometric estimation of the stochastic processes.
Aims:	This course aims at understanding the basic principles of pricing. Students are expected to improve their skills for solving the problems and writing their own codes for the estimation of the parameters and programming the pricng algorithms.
Outline:	WEEK 1: Review of the pricing for basic financial instruments and programming: Futures, Bonds, Swaps, FRA, FRN, etc…… WEEK 2: Review of the basic concepts in financial math: Binomial Market Model, Gaussian Market Model, Martingale Approach to Contingent Claim Pricing, PDE approach to Contingent Claim Pricing, Black-Scholes Equation, Term Structure Equation, Girsanov Theorem, Feynman Kac Theorem. WEEK 3: Monte Carlo methods for pricing and sensitivities WEEK 4-5: Estimation of Gaussian Stochastic Processes: Discrete and continuous time estimation of Brownian motion and Interest rate models. Calibration, LE, Generalized Method of Moments, Simulated Method of Moments-Efficient Method of Moments, Kalman Filter WEEK 6: Estimation of basic stochastic volatility and jump diffusion models WEEK 7: Options with closed form solutions: Pricing and Sensitivities , Vanilla Options, Exotic Options (Asian, Lookback, Barrier, Digital Options etc….) Bond Options WEEK 8: Implementation of Finite Difference methods: Pricing and Sensitivities WEEK 9-10. Implementation of Tree Approaches: Pricing, Sensitivities Parameter estimation Cox-Ross-Rubenstein, Black-Derman-Toy, Black-Karasinski, Hull-White, HJM WEEK 11-12: Projects
Suggested Textbooks:	Christian Gourieroux, Joann Jasiak, *Financial Econometrics: Problems, Models, and Methods* Peter G. Zhang, *Exotic Options: A Guide to Second Generation Options,* Paul Glasserman, *Monte Carlo Methods in Financial Engineering* Paul Wilmott, *Paul Wilmott on Quantitative Finance* John C. Hull, *Options, Futures and Other Derivatives* Paolo Brandimarte, *Numerical Methods in Finance and Economics: A MATLAB-Based Introduction*

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Adaptive Finite Elements and Optimal Control**
Course Code:	**IAM 762**
Credit:	(3-0)3
Instructor's Name:	Prof. Dr. Bülent Karasözen (bulent@metu.edu.tr)
Prerequisites:	Consent of the instructor.
Content:	Adaptive Finite Elements and Optimal Control
Aims:	Introduction to optimization and control problems with pde's
Learning Outcomes:	At the end of the course, student should be familiar wit the research topics related to the area and can start with their PhD thesis.
Outline:	Simple Model Problem Finite element discretization of elliptic PDEs Explicit a posteriori error estimates Implicit a posteriori error estimates The equilibrated residual method Examples of optimal control Optimal control of linear quadratic elliptic problems Optimal control of semi-linear quadratic elliptic problems
Course Material	M. Ainsworth and J.T. Oden, A pestoriori Error Estimation in Finite Element Analysis, Wiley, 2000 I. Babuska and T. Strouboulis, The Finite Element Method and its Reliability, Clarendon Press, Oxford, 2001 F. Tröltzsch, Optimale Steuerung partieller Di®erentialgleichungen, Vieweg, Wiesbaden, 2005 R. Verfürth, A Review of A Posteriori Estimation and Adaptive Mesh-Re¯nement Techniques,Wiley-Teubner, New York, Stuttgart, 1996
Supplementary Material	R.H.W Hoppe, Lecture Notes "Finite Elements" R.H.W. Hoppe, Lecture Notes "Optimization of Partial Differential Equations "

2007–2008 Güz Dönemi

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics : Pairing-Based Cryptography**
Course Code:	**IAM 713**
Credit:	(3-0)3
Instructor's Name:	Prof. Dr. Ersan Akyıldız (ersan@metu.edu.tr)
Prerequisites:	IAM 505 and Consent of the Instructor
Content:	Pairings in Elliptic Curve Cryptography: Tate pairing, Weil pairing,. Applications and Computational problems from pairings. Cryptography from pairings.
Aims:	The aim of this course is to study 1. Schoof and Schoof-Atkin -Elkin's algorithms to compute the number of points of an Elliptic Curve , 2. Elliptic curve factorization and primality test, 3. Pairings in Elliptic Curves Crytography. We shall introduce The Weil and Tate pairing on elliptic curves and study the applications and computional problems from pairings. We will also discuss how pairings are used to construct a wide range of cryptographic schemes, protocols and infrastructures supporting the use of public-key cryptography.
Learning Outcomes:	L.C.Washington, Elliptic Curves, Number Theory and Cryprography, Chapman&Hall/CRC I.Blake,G.Seroussi and N. Smart, Advances in Elliptic Curves in Cryptography, London Math.Soc. Lec.Note Series. No.317, 2004, QA 76.9 .A.25. A375
Suggested Textbooks:	Blake,G.Seroussi and N. Smart, Elliptic Curves in Cryptography, London Math.Soc. Lec.Note Series. No.256, 1999, QA 76.9 .A.25.B57 Henri Cohen and Gerhard Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman &Hall/CRC, QA 567.2. E 44H36, 2005

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Sequnce Design and Rings**
Course Code:	**IAM 715**
Credit:	**(3-0)3**
Instructor's Name:	Prof. Dr. Ferruh Özbudak (ozbudak@metu.edu.tr)
Prerequisites:	Consent of the instructor
Content	Finite fields and finite rings, Sequnces, power series, Linear feedback shift registers and linear recurrences, Algebraic feedback shift register sequences, Pseudo-random sequences, Correlation, Special types of good sequences, Sequence synthesis, Some codes over rings
Aims:	To provide basic background on finite commutaive rings and their applications in cryptography and related areas.
Learning Outcomes:	To learn basic techniques in finite fings, properties of sequences in application to coryptography and related area and some design techniques.
Suggested Textbooks:	1. Z.-X. Wan, "Lectures on finite fields and Galois rings", World Scientific, 2003. 2. B. R. McDonald, "Finite rings with identity", Marcel Dekker, 1974. 3. G. Bini, F. Flamini, "Finite commutative rings and their applications", Kluwer, 2002. 4. M. Goresky, A. Klapper, "Algebraic shift register seqeunces", draft book in preparation, 2007.
Outline:	• Finite fields and finite rings • Sequnces, power series • Linear feedback shift registers and linear recurrences • Algebraic feedback shift register sequences • Pseudo-random sequences • Correlation • Special types of good sequences • Sequence synthesis
Resourses:	The textbooks listed above and various reserach articles which will be mentioned during the course.

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Cryptological Characteristics of Boolean Function and S-Boxes**
Course Code:	**IAM 717**
Credit:	(3-0)3
Instructor's Name:	Assoc. Prof. Dr. Melek Yücel (yucel@eee.metu.edu.tr)
Prerequisites:	Consent of the instructor
Content	The primary focus of this course will be on characteristics and the constructions of Boolean functions and S-boxes. Course will mainly cover what security properties are desirable in such functions, how to properly obtain these properties, and how to design functions satisfying given properties. After taking the course, students should also have an overview of block cipher and stream cipher design and evaluation. Boolean functions, nonlinearity, diffusion, confusion, avalanche, strict avalanche criteria. Measures of main characteristics and tradeoffs. S-box construction. Structural and statistical evaluation of cipher systems
Suggested Textbooks:	• Joan Daemen, Cipher and Hash Function Design, Strategies, Doctoral dissertation Some relevant papers • A.J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography CRC Press, 1996. • M.J.B.Robshaw: Stream Ciphers. Technical Report TR-701, 2.0, RSA Laboratories, July 1995. • S.Sağdıçoğlu: Cryptological Viewpoint of Boolean Functions, M.Sc. Thesis, METU, 2003 • H.C.A van Tilborg. An introduction to Cryptology. Kluwer Academic Publisher, Boston, 1988.
Outline:	• Boolean functions (functions defined on GF(2)n), truth table, algebraic normal form, sequence of a function, Sylvester-Hadamard matrices, linear and affine functions, Walsh transform • Nonlinearity, measures of nonlinearity • Completeness, avalanche, strict avalanche and global avalanche criteria • Correlation immunity, resiliency • S-boxes, characteristics of S-boxes • Tradeoffs between degree, nonlinearity, SAC and resiliency of a booloean function • Construction of S-boxes • Cryptographic properties of functions defined on GF(2n) • Structural evaluation of block ciphers • Structural evaluation of stream ciphers • Statistical methods of evaluating cipher systems

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Numerical Algorithms with Financial Applications**
Course Code:	**IAM 749**
Credit:	(2-2)3
Instructor's Name:	Dr. Ömür Uğur (ougur@metu.edu.tr)
Prerequisites:	**Consent of the instructor**. (Knowledge of a programming language, preferably MATLAB, is a must. Knowledge of basic financial concepts is an advantage)
Content:	Fixed-income securities, basic portfolio optimization, binomial method for options; Ito process and its applications in stock market, Black-Scholes equation and its solution; random numbers, transformation of random numbers and generating normal variates, Monte Carlo integration, pricing options by Monte Carlo simulation, variance reduction techniques, quasi-random numbers and quasi-Monte Carlo simulation; introduction to finite difference methods, explicit and implicit finite difference schemes, Crank-Nicolson method, free-boundary value problems for American options.
Aims:	The main objective of the course is to introduce some numerical algorithms that are commonly used in financial applications. Moreover, to introduce basic options and their valuations both theoretically and numerically.
Outline:	The following outline is just a rough one, it may slightly change during the semester. 1. Fixed-Income Securities 2. Portfolio Optimization 3. Options, and the Binomial Model 4. Stochastic Differential Equations 5. Ito Processes and Applications in Stock Market 6. The Black-Scholes Equation, derivation and the Greeks 7. Random Numbers and Transformation of Random Variables 8. Monte Carlo (MC) Integration and Option Pricing by MC simulation 9. Variance Reduction Techniques 10. Introduction to Partial Differential Equations (PDEs) and Finite Difference Methods 11. An Explicit Method and An Implicit Method 12. Crank-Nicolson Method 13. Some Advanced Topics (includes quasi Monte Carlo Simulation and Free Boundary Value Problems)
Learning Outcomes:	Students are expected to gain, beside the theoretical concepts, programming skills that are related to option pricing as well as optimization.
Suggested Textbooks:	The lecture notes, mainly based on the following references, will probably be available to students. 1. Brandimarte, P., Numerical Methods in Finance: A MATLAB-Based Introduction, John Wiley & Sons, Inc., 2002 2. Seydel, R., Tools for Computational Finance, Springer-Verlag, 2002
Resources:	MATLAB, Financial Toolbox, Optimization Toolbox.

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Functional Analysis**
Course Code:	**IAM 781**
Credit:	(3-0)3
Instructor's Name:	Prof. Dr. Şafak Alpay (safak@metu.edu.tr)
Prerequisites:	Properties of real numbers,limitsand convergence of sequences of numbers,exponential and logarith function,continuity and uniform continuity of functions,intermidiate value theorem,Hölder and Lipschitz continuity,differentiabilty,and differentiation rules
Content:	Basic analysis , Banach spaces in particular L^p spaces,Sobelev spaces
Aims:	The students will be equippedwith sufficient knowledge of analysis to pursue their own reseach
Learning Outcomes:	Same as in "aims"
Suggested Textbooks:	J.Jost.Postmodern analysis Springer Universitext,1998 T.Terzioğlu: Fonksiyonel Analizin Yontemleri Matematik Vakfı T.Terzioğlu :Introduction to Real Analysis.Matematik Vakfı
Outline:	Week1.Banach Spaces and Banach fixed point Theorem Week2.Integrals and ODEs Week3.Metric spaces Week4.Differential calculus in R^n Week5:Implicit Function Theorem and Applications Week6: System of ODEs Week7:Semi continous functions Week8:Lebesgue integrals of semi continuous functions Week9 Lebesgue integrable functions Week 10:Fubini Therem Week11:Convergence Theorem of Lebesgue integrable functions Week 12Jensen's inequality and Egorov Theorem Week 13 L^p spaces Week14 Weak derivatives and Sobelev spaces

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Special Topics: Spatial Optimization**
Course Code:	**IAM 761**
Credit:	3(3-0)
Instructor's Name:	Hayri Önal, (h-onal@uiuc.edu)
Prerequisites:	An introductory course in linear programming
Content:	**Linear Programming**, simplex method, LP duality, formulations of prototype spatial optimization problems, transportation and transshipment problems ; **General Algebraic Modeling System** (GAMS), programming basics ; **Integer programming**, Branch and bound method, formulations of prototype IP problems in spatial optimization, modeling land use and land/water conservation, facility location problem, traveling salesman problem, vehicle routing problem, set covering and maximal covering problems and their applications in spatial optimization, the basic conservation reserve design problem; **Nonlinear Programming**, Kuhn-Tucker optimality conditions, market equilibrium analysis with endogenous prices, finding multi-market multi-region (spatial) equilibria using nonlinear optimization; **Graphs and Networks,** basics of graph theory and network flows, minimum spanning trees, the Steiner tree problem, applications of graphs and networks to designing conservation reserve networks with spatial considerations, in particular designing compact reserves and reserves with minimum boundary, reserve connectivity and fragmentation.
Aims:	The course presents models and modeling techniques used for various types of spatial optimization problems and a state-of-the art algebraic modelıng language for solving optimization problems.
Learning Outcomes:	The students will learn modeling techniques to address various types spatial optimization problems faced in practice and how to program and solve optimization problems using an optimization software.
Suggested Textbooks:	Instructor's class notes and various articles published in scientific journals. A complete list of journal articles will be provided.
Outline:	Weeks 1-2: Linear Programming and Applications in Spatial Optimization Week 3: Modeling and programming with GAMS Weeks 4-6: Integer Programming and Applications in Spatial Optimization Weeks 7-8: Nonlinear Programming Applications in Spatial Optimization Weeks 9-12: Graphs and Networks, Applications in Spatial Optimization Weeks 13-14: Term paper presentations and group discussion
Resources:	MS **Bazaraa**, JJ Jarvis, and HD Sherali. Linear Programming and Network Flows. John Wiley & Sons, Chichester, 1990.

EK: 6
2007 YILINDA AÇILAN DERSLERİN LİSTESİ

2006–2007 II. Döneminde verilen dersler

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Kriptografi	IAM 502	Stream Ciphers	Ali Doğanaksoy	19	2	21
	IAM 504	Public Key Cryptography	Emrah Çakçak	18	3	21
	IAM 512	Block Ciphers	Melek Yücel	11	-	11
	IAM 711	Special Topics: Elliptic Curve Cryptography	Ersan Akyıldız	9	-	9
	IAM 712	Special Topics: Applications of Finite Fields to Cryptography	Emrah Çakçak	20	-	20

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Bilimsel Hesaplama	IAM 562	Introduction to Scientific Computing II	Hakan Öktem	8	3	11
	IAM 566	Numerical Optimization	G.W. Weber	7	11	18
	IAM 570	Hybrid Systems	Hakan Öktem	8	-	8
	IAM 571	Applications of Differential Quadrature Method in Engineering	Münevver Tezer	1	6	7
	IAM 664	Inverse Problems	G.Wilhelm Weber	6	7	13
	IAM 762	Special Topics: Adaptive Finite Elements and Optimal Control	Bülent Karasözen	1	3	4

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Finansal Matematik	IAM 520	Financial Derivatives	Seza Danışoğlu	20	1	21
	IAM 522	Stochastic Calculus for Finance	Azize Hayfavi	16	3	19
	IAM 524	Financial Economics	Esma Gaygısız	22	1	23
	IAM 543	Regulation and Supervision of Risks	Coşkun Küçüközmen	12	1	13
	IAM 583	Pension Fund Mathematics	Ömer Gebizlioğlu	8	-	8
	IAM 611	Numerical Methods for Financial Models	A.Devin Sezer	2	-	2
	IAM 612	Financial Modeling with Jump Processes	Hayri Körezlioğlu	5	-	5
	IAM 746	Special Topics: Actuarial Risk Theory	Fatih Tank	6	-	6
	IAM 747	Special Topics: Quantitative Finance I	Kasırga Yıldırak	7	1	8

2007–2008 I. Döneminde verilen dersler

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Kriptografi	IAM 501	Introduction to Cryptography	Ali Doğanaksoy	20	3	23
	IAM 503	Applications of Finite Fields	Emrah Çakçak	19	1	20
	IAM 505	Elliptic Curves in Cryptography	Emrah Çakçak	11	-	11
	IAM 519	Basic Mathematics for Cryptography	Abdürrahim Yılmaz	3	-	3
	IAM 530	Elements of Statistics and Probability	Ayşen Akkaya	17	3	20
	IAM 713	Special Topics: Pairing-Based Cryptography	Ersan Akyıldız	3	-	3
	IAM 715	Special Topics: Cryptography and Coding Theory	Ferruh Özbudak	12	-	12
	IAM 717	Cryptological Characteristics of Boolean Function and S-Boxes	Melek Yücel	10	-	10

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Bilimsel Hesaplama	IAM 557	Statistical Learning and Simulation	G.W.Weber	11	-	11
	IAM 561	Introduction to Scientific Computing I	Hakan Öktem	11	10	21
	IAM 564	Basic Algorithms and Programming	B. Karasözen	8	-	8
	IAM 567	Mathematical Modelling	Hakan Öktem	10	3	13
	IAM 665	Advanced Continuous Optimization	G. W. Weber –B. Karasözen	11	1	12
	IAM 781	Special Topics: Functional Analysis	Ş. Alpay	4	2	6

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Finansal Matematik	IAM 521	Financial Management	A.Oran-S.Danışoğlu-N.Güner	16	2	18
	IAM 526	Time Series Applied to Finance	Coşkun Küçüközmen	22	1	23
	IAM 530	Elements of Statistics and Probability	Ayşen Akkaya	17	3	20
	IAM 541	Probability Theory	Azize Hayfavi	19	3	22
	IAM 544	Financial Risk Assessment	Kasırga Yıldırak	12	3	15
	IAM 556	Simulation	İnci Batmaz	6	2	8
	IAM 557	Statistical Learning and Simulation	G.W.Weber	11	-	11
	IAM 582	Life Insurance Mathematics	Fatih Tank	4	-	4
	IAM 584	Advanced Actuarial Mathematics	Ömer Gebizlioğlu	4	-	4
	IAM 745	Special Topics Stochastic and Deterministic Optimal Control with Applications to Finance	A.Devin Sezer	1	2	3
	IAM 749	Special Topics: Numerical Methods with Financial Applications	Ö. Uğur	11	1	12