ORTA DOĞU TEKNİK ÜNİVERSİTESİ
UYGULAMALI MATEMATİK ENSTİTÜSÜ

RAPOR

2005

İÇİNDEKİLER

ÖZET BİLGİLER

(2004-2005 II. Dönem ve 2005-2006 I. Dönem)

ENSTİTÜNÜN PROGRAMLARI

Bilimsel Hesaplama
Tezli Yüksek Lisans
Doktora

Finansal Matematik
Tezli Yüksek Lisans
Tezsiz Yüksek Lisans
Hayat Sigortası Opsiyonu
Doktora

Kriptografi
Tezli Yüksek Lisans
Tezsiz Yüksek Lisans
Doktora

AKADEMİK PERSONEL

Enstitümüzün Kadrolu Akademik Personeli:

Profesör	Y. Doçent	Öğretim Görevlisi	DOSAP	Araştırma Görevlisi
2	**1**	**2**	**3**	**15**

Bağlantılı Öğretim Üye Sayısı
57

Bağlantılı Öğretim Üyelerinin Bölümlere/Kurumlara göre Dağılımı

ODTÜ	
Matematik Bölümü	**10**
Elektrik-Elektronik Mühendisliği Bölümü	**6**
İşletme Bölümü	**4**
İktisat Bölümü	**4**
Biyoloji Bölümü	**4**
Gıda Mühendisliği Bölümü	**2**
Kimya Mühendisliği Bölümü	**2**
Kimya Bölümü	**2**
Beden Eğitimi ve Spor Bölümü	**1**
Endüstri Mühendisliği Bölümü	**1**
Enformatik Enstitüsü	**1**
Fizik Bölümü	**1**
İstatistik Bölümü	**1**
Jeodezi ve Coğrafi Bilgi Teknolojileri	**1**
Makine Müh. Bölümü	**1**

ÜNİVERSİTELER	
Ankara Üniversitesi	
İstatistik Bölümü	**1**
Matematik Bölümü	**1**
Bahçeşehir Üniversitesi	**1**
Hacettepe Üniversitesi	
İstatistik Bölümü	**1**
Illinois State University	
Department of Mathematics	**1**
İstanbul Ticaret Üniversitesi	**1**
İzmir Yüksek Teknoloji Enstitüsü	
Matematik Bölümü	**1**
Koç Üniversitesi	
İşletme-Ekonomi Bölümü	**1**
College of Engineering	**1**
TOBB Ekonomi ve Teknoloji Üniversitesi	
Bilgisayar Bölümü	**1**

KURUMLAR	
T.C. Merkez Bankası	**1**
Toros Menkul Kıymetler A.Ş.	**1**
TÜBİTAK-UEKAE	**2**
DİĞER	**2**

Enstitümüzü 2005 Yılında Kısa Süreli Ziyaret Eden Yabancı Öğretim Üye Sayısı : 12*

Enstitümüz Kanalıyla Yurt Dışı Araştırma Kurumlarını Ziyaret Eden UME Bağlantılı

Öğretim Üye Sayısı: 11
Öğretim Elemanı Sayısı: 2
Araştırma Görevlisi Sayısı: 1

İDARİ PERSONEL

Sekreter : 1 **İdari Amir : 1**

* Enstitümüzü 2005 yılında kısa süreli olarak ziyaret öğretim üyelerinin listesi **Ek 3**'de verilmiştir.

ÖĞRENCİ BİLGİLERİ

Enstitümüzün Toplam Öğrenci Sayısı:
134

2005 Yılında Mezun Olan Öğrenci Sayısı*:
34

Enstitümüz Öğrencilerinin Programlara göre Dağılımı

Anabilim Dalı	Yüksek Lisans	Doktora	Bilimsel Hazırlık	Mezun
Bilimsel Hesaplama	**16**	**7**	**-**	**5**
Finansal Matematik	**27**	**8**	**10**	**12**
Finansal Matematik Hayat Sigortası Opsiyonu	**15**	**-**	**-**	**9**
Kriptografi	**18**	**24**	**9**	**8**
Toplam:	**76**	**39**	**19**	**34**

2005 yılında Kayıt Yaptıran Öğrencilerin B.S. Derecelerini Aldıkları Bölümlere Göre Dağılımları**

MATH	STAT	CENG	ECON	BA	EE	IE	PHYS
30	**12**	**8**	**5**	**4**	**4**	**2**	**1**

UME Derslerini Alan Öğrencilerin Bölümlere Göre Dağılımı***

Dönem	UME	MATH	PHYS	EE	IE	CENG	ECON	BIOL	GENE	ENVE	MI	METE	IS	AEE	MINE	ES	ME	CHE	STAT	CE	GGIT	FDE	Özel Öğr.
2004-2005 II	**142**	**8**	**6**	**5**	**15**	**3**	**4**	**-**	**-**	**-**	**1**	**2**	**1**	**1**	**-**	**1**	**-**	**1**	**-**	**1**	**-**	**-**	**10**
2005-2006 I	**214**	**10**	**2**	**7**	**-**	**3**	**3**	**4**	**1**	**-**	**-**	**-**	**1**	**-**	**2**	**1**	**1**	**1**	**2**	**1**	**-**	**1**	**11**

* Bu öğrencilerin listesi **Ek 5**'de verilmiştir.
** Bölüm isimlerinde ODTÜ Katalogunda ki kısaltmalar kullanılmıştır.
***Enstitümüzde 2004-2005 II ve 2005-2006 I. Döneminde verilen derslerin listesi **Ek 7**'da verilmektedir.

Dönemsel Ders İstatistikleri:

	Verilen Ders Sayısı	Toplam Öğrenci Sayısı	Ders Başına Verilen Not Sayısı
2004-2005 II.Dönem	16	201	13
2005-2006 I.Dönem	25	266	11

Öğrenci Başarı Durumları

	2004-2005 II.Dönem				2005-2006 I.Dönem			
	Başarılı	**Başarısız**	**Atılan**	**İzinli**	**Başarılı**	**Başarısız**	**Atılan**	**İzinli**
Kriptografi (Bil.Haz.)	-	-	3	-	7	2	-	-
Kriptografi (İng.Haz.)	-	-	-	-	-	-	-	-
Kriptografi (M.Sc.)	15	2	-	-	14	4	-	-
Kriptografi (Ph.D.)	16	-	-	-	20	3	1	1
Bilimsel Hesaplama (M.Sc.)	11	3	1	-	11	3	1	2
Bilimsel Hesaplama (Ph.D.)	4	-	-	-	5	1	1	-
Finansal Matematik (Bil. Haz.)	-	4	-	-	6	2	1	-
Finansal Matematik(M.Sc.)	23	6	1	3	18	3	-	5
Finansal Matematik (Ph.D.)	2	-	-	-	4	3	1	-
Hayat Sigortası (Bil. Haz.)	-	-	-	-	-	-	-	-
Hayat Sigortası (M.Sc.)	10	6	2	1	10	3	1	-
TOPLAM	**81**	**21**	**7**	**4**	**95**	**24**	**6**	**8**

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	1	1	-
Ondokuz Mayıs Üniversitesi SAMSUN	-	-	-	-	-	-	1	-	-	1	-	-
Kırgız Milli Üniversitesi	-	-	-	-	-	-	1	-	-	1	-	-
Kırgız Türkiye Manas Üniversitesi	-	-	-	-	-	-	-	1	-	1	-	-

ARAŞTIRMA FAALİYETLERİ

Yurtdışı Makale ve Tebliğler*

Yurtdışında basılmış makale:	Uluslararası Toplantılarda Sunum:	Uluslararası Toplantılarda Tebliğ
11	**13**	**5**

Yurtiçi Makale ve Tebliğler*

Yurtiçi Toplantılarda Sunum:	Yurtiçi Toplantılarda Tebliğ
2	**12**

Raporlar*

Yurtdışı Rapor
3

UME Preprint Serisi (IAM Preprint Series)*: 47
(www.iam.metu.edu.tr/research Preprint Series)

* Yayın/tebliğlerinde UME bağlantılarını belirtmiş öğretim üyelerimizin araştırma faaliyetleri dikkate alınmıştır. Bu makalelerin ve Preprintlerin listesi **Ek 1**'de verilmektedir.

DEVAM EDEN PROJELER

DPT	Kriptografi Konusunda Araştırma, Geliştirme; Algoritma Tasarımı, Analizi ve Uygulanması Projesi. Başlama 2004 -
DAAD Projesi (IAM, Kaiserslautern ve TU Darmstadt)	Cooperation in the Field of Financial and Insurance Mathematics. Başlama 2004 -
European Science Foundation Projesi	Advanced Mathematical Methods for Finance. Başlama 2004 -
TÜBİTAK Bütünleşik Doktora Programı Projesi	Sürekli Optimizasyon Yöntemleri ve Uygulamaları. Başlama 2004 -
BAP 1	Gelişmekte olan Finans Piyasaları Çerçevesinde Bankalarda Risk Yönetimi ve Sermaye Dağılımı. Başlama 2004 -
BAP 1	Türkiye Finans Piyasalarına Uyum Sağlayacak Risk Modelleri Araştırma, Geliştirme Ve Uygulamaları Projesi. Başlama 2004 -

2005 YILINDA BAŞLATILAN PROJELER

TÜBİTAK araştırma projesi	Nükleer füzyon reaktör problemlerinin sınır elemanları ve sonlu elamanlar yöntemleri ile çözümü
NSF- TÜBİTAK INT projesi.	Development of Modeling and Optimization Tools for Hybrid Systems
TÜBİTAK Kariyer Projesi	Modeling Multistationary Processes by Using Hybrid System Formulation: A study with Priority on Functional Genomics

DÜZENLENEN TOPLANTILAR

- **Workshop on Sustainable Living in Rural Areas of Turkey**
  (7-21 Mart 2005, Ankara)
- **Türk-Alman Yaz Akademisi**
  (28 Ağustos-3 Eylül 2005, İzmir)
- **I. Ulusal Kriptoloji Sempozyumu**
  (18-20 Kasım 2005, Ankara)

ULUSLARARASI PROTOKOLLER

Universitat Kaiserslautern and Middle East Technical University Instute of Applied Mathematics	Cooperation in the Field of Financial and Insurance 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 of the Middle East Technical University (IAM-METU)**	Cooperation in the fields of Financial Mathematics, and Cryptography
University of the Aegean, Greece (Department of Statistics and Actuarial Science), Middle East Technical University (Institute of Applied Mathematics)	Cooperation in the fields of Financial Mathematics, Actuarial Sciences and Establishment of a Joint Doctoral Program
General Memorandum of Agreement on Cooperation Between Institute of Mathematics of The Polish Academy of Sciences and The Institute of Applied Mathematics and Department Mathematics and Middle East Technical University	Memorandum on Extending and Strengthening Links Beetween Polish Academy of Sciences and the Department of Mathematics and Institute of Applied Mathematics
Turkish-French University and Scientific Cooperation Projects, Laboratoire de Mathématiques et Applications Université de La Rochelle and Institute of Applied Mathematics, Middle East Technical University, Ankara	Exchange of know-how in Financial Mathematics, Development of common teaching and research programs, Joint participation to European research projects.

UYGULAMALI MATEMATİK ENSTİTÜSÜ

2002 yılında kurulan Uygulamalı Matematik Enstitüsü, Finansal Matematik, Kriptografi, Bilimsel Hesaplama programlarıyla yüksek lisans ve doktora; Finansal Matematik Hayat Sigortası Opsiyonu'yla da yüksek lisans eğitimi vermektedir. Misyonunu;

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 yayın yapmak.

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

olarak belirlemiştir.

ENSTİTÜNÜN İNSAN KAYNAKLARI

- UME'nin **akademik kadrosu** 31 Aralık 2005 tarihi itibari ile **2 Profesör, 4 Yardımcı Doçent, 2 Öğretim Görevlisi ve 15 Araştırma Görevlisinden** oluşmaktadır.

Öğretim Elemanları
Hayri Körezlioğlu
Gerhard- Wilhelm Weber
Hakan Öktem
Emrah Çakçak
Ömür Uğur

DOSAP
Pakize Taylan
(Dicle Üniversitesi)
Rengin Ak
(100. Yıl Üniversitesi)
Ş. Kasırga Yıldırak
(Trakya Üniversitesi)

Araştırma Görevlileri
Sedat Akleylek (ÖYP, Samsun)
Zeynep Sırma Alparslan (ÖYP, Isparta)
Derya Altıntan (ÖYP, Konya)
Derviş Bayazıt (YÖK Bursu ile yurtdışında)
Rita İsmailova (ÖYP, Kırgızistan)
Ayşegül İşcanoğlu (ÖYP, Konya)
Turgut Hanoymak (ÖYP, Van)
Barış Bülent Kırlar (ÖYP, Isparta)
Süreyya Özöğür
Zülfükar Saygı
Oktay Sürücü
Mesut Taştan (ÖYP, Van)
Nurbek Baryk Ulu (ÖYP, Kırgızistan)
Çekdar Vakıfahmetoğlu
Yeliz Yolcu

BAĞLANTILI ÖĞRETİM ÜYELERİ

ORTA DOĞU TEKNİK ÜNİVERSİTESİ

Matematik Bölümü	Marat U. Akhmet Ersan Akyıldız Muhammed Dabbagh Ali Doğanaksoy Tanıl Ergenç Bülent Karasözen Ebru Keyman Ferruh Özbudak Münevver Tezer Muhiddin Uğuz
Elektrik-Elektronik Mühendisliği Bölümü	F. Rüyal Ergül Nevzat G. Gençer Kemal Leblebicioğlu Yeşim Serinağaoğlu Doğrusöz Osman Sevaioğlu Melek Yücel
İşletme Bölümü	Nuray Güner Adil Oran Seza Danışoğlu Rhoades Engin Küçükkaya
İktisat Bölümü	Işıl Erol Esma Gaygısız Şaziye Gazioğlu Murat G. Kırdar
Biyoloji Bölümü	Meryem Beklioğlu Semra Kocabıyık Gülay Özcengiz İnci Togan
Gıda Müh.Bl.	Deniz Çekmecelioğlu Zümrüt Begüm Ögel
Kimya Bölümü	Ali Gökmen Mahinur Akkaya
Kimya Müh. Bl.	Gürkan Karakaş Yusuf Uludağ
Beden Eğitimi ve Spor Bl.	Feza Korkusuz
Endüstri Müh. Bl.	Yasemin Serin
Enformatik Enstitüsü	Erkan Mumcuoğlu
Fizik Bölümü	Yusuf İpekoğlu
GGIT	Şebnem Düzgün
İstatistik Bölümü	İnci Batmaz
Makine Müh. Bl.	Haluk Aksel

ÜNİVERSİTELER

ANKARA ÜNİVERSİTESİ **İstatistik Bölümü**	Ömer Gebizlioğlu
Matematik Bölümü	Ali Bülent Ekin
BAHÇEŞEHİR ÜNİVERSİTESİ	İrini Dimitriyadis
HACETTEPE ÜNİVERSİTESİ **İstatistik Bölümü**	Gül Ergün
ILLINOIS STATE UNIVERSITY **Mathematics**	Sevtap Selçuk Kestel
İSTANBUL TİCARET ÜNİVERSİTESİ	Çetin Kaya Koç
İZMİR YÜKSEK TEKNOLOJİ ENSTİTÜSÜ **Matematik Bölümü**	Ali İhsan Neslitürk
TOBB ETU **Bilgisayar Bölümü**	Ali Yazıcı
KOÇ ÜNİVERSİTESİ **İşletme ve Ekonomi Bölümü**	Sumru Altuğ
Mühendislik Fakültesi	Metin Türkay

KURUMLAR

TCMB	C.Coşkun Küçüközmen
Toros Menkul Kıymetler A.Ş.	Ali Veysoğlu
TÜBİTAK-UEKAE	İsmail Güloğlu Orhun Kara

DİĞER

Azize Hayfavi
Gülçin Sağdıçoğlu Celep

- UME'nin **idari personeli** bir sekreter ve bir idari amirden oluşmaktadır.

Sekreter: Nejla Erdoğdu **İdari Amir:** Saffet Aykın

UME'NİN 2005 YILI FAALİYETLERİ

Bu rapor 2005 takvim yılı (**2004-2005 II. ile 2005-2006 I. Dönemi**) Uygulamalı Matematik Enstitüsü faaliyetlerini kapsamaktadır.

Kuruluşundan itibaren Matematik Bölümü M-205 ve M-204 nolu odalarda faaliyetini sürdüren Enstitümüz
Temmuz ayında Fen Edebiyat Fakültesi (S Binası) ikinci katında bulunan yerleşkesine taşınmıştır. Enstitümüzün kurucularından ve ilk müdürü olan Prof. Dr. Aydın Aytuna'nın Ağustos ayında emekli olması nedeniyle yerine Prof. Dr. Ersan Akyıldız müdür olarak atanmıştır. Enstitümüzün yerleşkesinin açılışı Rektörümüz Prof. Dr. Ural Akbulut'un katılımıyla 20 Eylül 2005 tarihinde yapılmıştır.
(Detaylı bilgi için: http://www.iam.metu.edu.tr/announce/sunum.ppt)

Enstitümüze ilk defa bu yıl Doktora Sonrası Araştırma Programı çerçevesinde (DOSAP) 3 yeni öğretim üyesi katılmıştır. Bu dönemde ki bağlantılı öğretim üyesi sayımız ise 50'den 57'ye çıkmıştır. Öğretim Üyesi Yetiştirme Programı (ÖYP) çerçevesinde ise, 9 asistan göreve devam etmekte olup bir asistanımız Amerika Birleşik Devletleri Florida State Üniversitesi'nde YÖK burslusu olarak bulunmaktadır.

Uygulamalı Matematik Enstitüsü'nde 2004-2005 Akademik yılının II. döneminde **16**, 2005-2006 akademik yılının ilk döneminde ise **25** ders açılmıştır. Enstitümüzün eğitim etkinlikleri, açılan dersler ve bu dersleri alan öğrenciler ile ilgili bilgileri içeren öğrenci istatistikleri ayrıntılı olarak **Ek 4**'de verilmiştir.

Enstitümüzdeki ilk yıllarını tamamlayan Finansal Matematik öğrencileri, programları gereği, çeşitli finans kuruluşlarında **"Yaz Stajı"** yapmışlardır. Öğrencilerin staj yaptığı kurumlar **Ek 8**'de verilmiştir.

Enstitümüzde, araştırma gruplarının kendi seminerleri dışında, üç ayrı kategoride seminerler düzenlenmiştir. Bunlar: **Enstitü Genel Seminerleri, Uygulayıcılar Seminerleri ve SIAM-IAM Öğrenci Seminerleri'**dir. 2005 yılı UME seminerlerinin bir dökümü **Ek 2**'de verilmiştir. Konuşmaların özetlerine enstitü web sayfasından (www.iam.metu.edu.tr/seminerler) ulaşılabilinir.

IAM Preprint Serisi'nin sayısı, 2005 yılı sonu itibariyle 29'dan 47'ye ulaşmıştır (**Ek 1)** Bu preprintler, düzenli bir şekilde yurtdışında bulunan 40 civarında eğitim ve araştırma kurumuna gönderilmektedir. Ayrıca preprintlerimiz web sayfamıza da konulmaktadır.
(http://www.iam.metu.edu.tr/body1.php?PageId=120100)

Avrupa Yöneylem Derneklerinin üst kuruluşu olan **EURO**'nun çalışma gruplarından **EUROPT**'un (**EURO Working Group on Continuous Optimization**) eşbaşkanlığına Enstitümüz öğretim üyelerinden Prof. Dr. G.Weber 2005 yılında da devam etmiştir. **EUROPT**'un web sayfasına UME ev sahipliği yapmaktadır.

SIAM-IAM Öğrenci Topluluğu, **SIAM** (Society for Industrial and Applied Mathematics) ile bağlantılı olarak Amerika Birleşik Devletleri ve Kanada dışında kurulan ilk öğrenci grubu olma özelliğini taşımaktadır. Bu grubun 2005 yılı faaliyetleri aşağıda ayrıca ele alınacaktır.

Enstitümüzün programları ve araştırma gruplarının 2005 yılı faaliyetlerini, aşağıda ayrıntılı bir biçimde ele alacağız.

KRİPTOGRAFİ PROGRAMI

2005-2006 öğretim yılında UME Kriptografi programına basvuran 50 öğrenciden 31'i kabul edilmiş, ancak bunlardan 22'si programa kayıt yaptırmıştır. Yüksek lisans programına kabul edilen öğrencilerin LES puanları ortalaması 66.8, CGPA ortalaması 2.81/4.00, Doktora programına kabul edilen öğrencilerin LES puanları ortalaması 69.4, CGPA ortalaması 2.94/4.00'dir.

2005-2006 öğretim yılında programa kabul edilen öğrencilerin %77'si lisans derecesini ODTÜ'den almış ve bunların da%55'i Matematik Bölümü mezunlarıdır. Diğer öğrencilerin, lisans derecelerini aldıkları üniversite ve bölümleri aşağıda ki gibidir.
Üniversiteler:

- Bilkent Üniversitesi, Hacettepe Üniversitesi, Başkent Üniversitesi, Yıldız Teknik Üniversitesi, Çankaya Üniversitesi ve Ankara Üniversitesi.

Bölümler:

- Matematik, İstatistik, Bilgisayar Mühendisliği, Elektrik-Elektronik Mühendisliği ve İnşaat Mühendisliği.

2005 yılında Kriptografi doktora programında, Mayıs ayında yapılan doktora yeterlik sınavına giren 4 öğrenci de başarılı olmuş, Kasım ayında yapılan sınava giren 2 öğrenciden ise 1'i başarılı olmuştur.

Kriptografi Anabilim dalında doktora ve tezli/tezsiz yüksek lisans programları mevcuttur. 2005 yılında 2 öğrenci tezli, 6 öğrenci ise tezsiz yüksek lisans programından mezun olmuşlardır. **Ek 5**'de yüksek lisans tezleri ve bitirme projelerinin başlıklarını bulabilirsiniz.
(Özler için: http://www.iam.metu.edu.tr/body1.php?PageId=160500)

KONFERANS KATILIMLARI

- **Elif Saygı, Meltem Sönmez Turan ve Zülfükar Saygı,** BFCA'05, Fransa Rouen, 7-9 Mart 2005.

- **Ersan Akyıldız ve Emrah Çakçak**, ASIACRYPT 2005, Chennai-Hindistan, 4-8 Aralık 2005.

- **Ersan Akyıldız ve Emrah Çakçak,** INDOCRYPT 2005, Bangalore-Hindistan, 10-12 Aralık 2005.

- **Ersan Akyıldız, Ali Doğanaksoy, Ferruh Özbudak, Muhiddin Uğuz, Melek Yücel, Meltem Sönmez Turan, Baha Güçlü Dündar, Faruk Göloğlu, Zülfükar Saygı, Fatih Sulak, Deniz Toz, Elif Saygı, Orhan Çetinkaya**, I. Ulusal Kriptoloji Sempozyumu, Ankara, 18-20 Kasım 2005.

- **Emrah Çakçak** , Journees Arithmetiques XXIV, Marseille, France, 2005.

- **Emrah Çakçak,** Arithmetic, Geometry and Coding Theory (AGCT 10), CIRM, Luminy, Marseille, France, Septembre 26-30, 2005.

YURT DIŞI İLİŞKİLER

- **Emrah Çakçak**, doktora sonrası çalışmalar, IML/Marseille/Fransa 14 Mart - 30 Eylül 2005.
- **Emrah Çakçak**, doktora sonrası çalışmalar, Universite Laval, Quebec, Canada 01 -31 Ekim 2005.
- **Prof. Dr. Ersan Akyıldız**, Darmstadt Teknik Üniversitesi, Almanya, 6-8 Haziran 2005.

PAYDAŞLARLA BAĞLANTILAR:

2005 yılında da Kriptografi anabilim dalı belirlenen paydaşları ile ilişkilerini sürdürmüştür. Bu kapsamda:

- **Türk Telekomünikasyon Kurulu** ile birlikte "Açık Anahtar Altyapısı Konusunda Araştırma Geliştirme ve Uygulamalar"başlıklı bir proje önerisi Tübitak'a sunulmuş ve bu projenin revizyonu istenmiştir.
- **TÜBİTAK- UEKAE** ile Akan Şifre sistemlerinin analizi ve tasarımı konusunda ortak proje üretmek için çalışmalar başlatılmıştır.
- **T.C. Başbakanlık** mensuplarına bir danışmanlık projesi oluşturma sürecine girilmiştir. Bu kapsamda "Kriptolojinin Temelleri" adlı bir seminer dizisi geliştirilmiştir. Dokuz ay süren eğitim ODTÜ-Sürekli Eğitim Merkezinde gerçekleştirilmiştir. (http://www.iam.metu.edu.tr/body1.php?PageId=100100)

YÜRÜTÜCÜLÜĞÜ YAPILAN PROJELER

DEVAM EDEN 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, Ebru Keyman, Emrah Çakçak.
Süresi: 1.1.2004-31.12.2006

TAMAMLANAN PROJELER:

Projenin Adı: Blok Şifre Sistemlerinin Analizi ve Değerlendirilmesi için bir Yazılım Paketinin Geliştirilmesi ve Yeni Blok Şifre Sistemlerinin Tasarımı (BAP-2003-07-05-01 "SAKDAT")
Yürütücüsü: Ali Doğanaksoy
Araştırmacıları: Muhiddin Uğuz, Kerem Kaşkaloğlu, Zülfikar Saygı, Meltem Sönmez Turan, Abdülkadir Altan, Elif Saygı, Senay Yıldız
Süresi: Ocak 2003- Haziran 2005

DÜZENLENEN ÇALIŞTAYLAR VE SEMİNERLER:

I. Ulusal Kriptoloji Sempozyumu

18-20 Kasım tarihleri arasında Uygulamalı Matematik Enstitüsü tarafından 1. Ulusal Kriptoloji Sempozyumu düzenlenmiştir. Bu Sempozyum, Kriptoloji konusunda Türkiyede düzenlenen ilk bilimsel toplantı olmuştur. Sempozyum, Rektörümüz Sayın Prof. Dr. Ural Akbulut ve Müdürümüz Sayın Prof. Dr. Ersan Akyıldız'ın konuşmaları ile başlatılmış ve yaklaşık 130 kişi dinleyici olarak katılmıştır. Sempozyumda Indian Statistical Institute'den Subhamoy Maitra "Cryptanalysis of Digital Watermarking" ve "Cryptographically Significant Boolean Functions", İstanbul Ticaret Üniversitesi'nden Çetin Kaya Koç "Cryptographic Engineering", ASELSAN Elektronik Sanayii ve Ticaret A.Ş. den Ali Yazıcı "Savunma Sanayiinde Kriptoloji Çalışmaları", TÜBİTAK UEAKE'den Olay Salcan "Türkiye'deki Kriptoloji Uygulamalarının Tarihçesi" konularında davetli olarak konuşma yapmışlar ve sunulan makale sayısı 19 olmuştur. Sempozyum TÜBİTAK ve ODTÜ'nün destekleriyle düzenlenmiştir. Detaylı bilgiler http://www.iam.metu.edu.tr/sempozyum adresinde bulunabilir.

ARAŞTIRMA GRUPLARI

AÇIK ANAHTAR ALTYAPISI (AAA) ARAŞTIRMA GRUBU

- 2004 yılının Ekim ayında "Public Key Infrastructure Research Group" adlı bir araştırma grubu kurulmuştur, bu grubun amacı "e-dönüşüm Türkiye" çerçevesinde projeler hazırlayarak kamu ve özel sektöre danışmanlık ve ürüne yönelik hizmetlerde bulunmaktır. Bu kapsamda Türk Telekomünikasyon Kurulu ile birlikte "Açık Anahtar Altyapısı Konusunda Araştırma Geliştirme ve Uygulamalar"başlıklı bir proje önerisini Tübitak'a sunmuştur.

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. AAA; gizlilik (**confidentiality**), bütünlük (**integrity**), kimlik belirleme (**authentication**) ve reddedememe (**non-repudiation**) fonksiyonlarını kullanıcıların dijital sertifika kullanması yolu ile gerçekleştirir. Üzerinde çalışan elektronik imza ile kişilerin ve/veya kurumların elektronik ortamda tanınmasını sağlar. (Daha fazla bilgi için: www.pki.iam.metu.edu.tr)

Grup üyeleri

Muhiddin UĞUZ (Koordinatör) (Matematik Bl./UME)	**Faruk GÖLOĞLU** (UME)	**Elif SAYGI** (UME)
Ersan AKYILDIZ (Matematik Bl./UME)	**H. Murat YILDIRIM** (Matematik Bl.)	**Meltem Sönmez TURAN** (UME)
Rüyal ERGÜL (Elektrik-Elektronik Bl./UME)	**Kadir ERDOĞAN** (Matematik Bl.)	**Ayşe Nurdan SARAN** (UME)
Ali DOĞANAKSOY (Matematik Bl./UME)	**Murat CENK** (UME)	**Fatih SULAK** (UME)
Zülfükar SAYGI (Koordinatör Yrd.) (UME)	**Atilla BEKTAŞ** (Webmaster) (UME)	**Çağdaş ÇALIK** (UME)
Feyza Taşkazan ERYOL (TÜBİTAK Bilten/UME)	**Oğuz YAYLA** (UME)	

BOOLE FONKSİYONLARI ÇALIŞMA GRUBU

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. Bu özellikler dengelilik, tam çığ ölçütü (strict avalanche criterion), yüksek nonlineerite, yüksek cebirsel derece, yüksek mertebede korelasyon bağışıklığı ve yüksek mertebede propagation kriteri. 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.

Uygulamalı Metematik Enstitüsü Boole Fonksiyonları Çalışma Grubu yukarıdaki açıklanan konular çerçevesindeki problemler üzerinde durmaktadır. Ayrıca grup üyeleri haftada yaklaşık üç gün değişik altgruplarda toplanmakta ve ayda bir bütün grup üyelerinin katılımıyla elde edilen gelişmeleri değerlendirmektedir.

Grup Üyeleri

Ali Doğanaksoy(Koordinatör)(Matematik Bl./UME)
İsmail Şuayip Güloğlu (TÜBİTAK-UEKAE/ UME)
Muhiddin Uğuz (Matematik Bl./UME)
Baha Güçlü DÜNDAR (UME)
Elif Saygı (UME)
Zülfükar Saygı (UME)
Faruk Göloğlu (UME)
Fatih Sulak (UME)
H. Murat Yıldırım (Matematik Bl.)
İsa Sertkaya (TÜBİTAK-UEKAE/UME)
Kayhan Uluer (TÜBİTAK-UEKAE)
M. Rıdvan Bakkal (TÜBİTAK-UEKAE)
Serhat Sağdıçoğlu (TÜBİTAK-UEKAE/UME)

Grup Web Sayfası: http://www.math.metu.edu.tr/bfwg

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.

Grup Üyeleri:
Ferruh Özbudak (Koordinatör), Ersan Akyıldız, Emrah Çakçak, Zülfükar Saygı, Murat Cenk.

AKAN ŞİFRE SİSTEMLERİ ÇALIŞMA GRUBU

Uygulamalı Matematik Enstitüsü 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. Ayrıca grup üyeleri haftada yaklaşık üç gün değişik altgruplarda toplanmakta ve ayda bir bütün grup üyelerinin katılımıyla elde edilen gelişmeleri değerlendirmektedir.

Grup Üyeleri

Ali Doğanaksoy(Koordinatör)(Matematik Bl./UME)	**Orhun Kara** (TÜBİTAK-UEKAE/ UME)	**Meltem Sönmez TURAN** (UME)
İsmail Şuayip Güloğlu (TÜBİTAK-UEKAE/ UME)	**Elif Saygı** (UME)	**Ayşe Nurdan SARAN** (UME)
Muhiddin Uğuz (Matematik Bl./UME)	**Zülfükar Saygı** (UME)	**Çağdaş ÇALIK** (UME)

YURT DIŞI YAYINLAR:

- **E. Saygı, Z. Saygı, M. Sönmez Turan, A. Doğanaksoy**, "Statistical Approach on the Number of SAC Satisfying Functions", BFCA'05, First Workshop on Boolean Functions: Cryptography and Applications, Rouen, France, 2005.

- **E.Çakçak, F. Özbudak**, Number of Rational Places of Subfields of the Function Field of the Deligne-Lusztig Curve of Ree Type, Acta Arith. 120, no.1, 79-106, 2005.

YURT İÇİ TEBLİĞLER:

- **D. Toz, A. Doğanaksoy, M. Sönmez Turan**, "Statistical Analysis of Block Ciphers", 1. Ulusal Kriptoloji Sempozyumu, 56-66, 2005.

- **A. Doğanaksoy, B. G. Dündar, F. Göloğlu, Z. Saygı, F. Sulak, M. Uğuz**, "Constructions of Highly Nonlinear Balanced Boolean Functions", 1. Ulusal Kriptoloji Sempozyumu, 79-84, 2005.

- **F. Göloğlu, M. D. Yücel**, "Necessary Conditions on Balanced Boolean Functions with Maximum Nonlinearity", 1. Ulusal Kriptoloji Sempozyumu, 106-111, 2005.

- **A. Doğanaksoy, S. Sağdıçoğlu, Z. Saygı, M. Uğuz**, "An Interpretation of Sums of Walsh Spectrum Powers of Boolean Functions", 1. Ulusal Kriptoloji Sempozyumu, 112-116, 2005.

- **A. Doğanaksoy, E. Saygı**, **"**On The Quadratic Feedback Shift Registers**"**, 1. Ulusal Kriptoloji Sempozyumu, 127-133, 2005.

- **M. Cenk ve F. Özbudak,** "Elliptic Eğri Kriptografi ve Aritmetiği", 1. Ulusal Kriptoloji Sempozyumu, 134-141, 2005.

- **F. Özbudak ve Z. Saygı**, **"**Constructions of Systematic Authentication Codes**"**, 1. Ulusal Kriptoloji Sempozyumu, 143-148, 2005.

- **A. Doğanaksoy, F. Göloğlu**, **"**On Lempel-Ziv Complexity of Sequences**"**, 1. Ulusal Kriptoloji Sempozyumu, 149-155, 2005.

- **H.M. Yıldırım ve E. Akyıldız**, **"**New Properties of IDEA ciphers Operations**"**, 1. Ulusal Kriptoloji Sempozyumu, 156-166, 2005.

- **O. Çetinkaya, A. Doğanaksoy,** "Electronic Voting Protocols Based on Blind Signatures", 1. Ulusal Kriptoloji Sempozyumu, 189-198, 2005.

BİLİMSEL HESAPLAMA PROGRAMI

Bilimsel Hesaplama programında 2005-2006 I. döneminde Doktora programı başlatılmış, temel ve seçmeli alanlardan oluşan doktora yeterlilik konuları belirlenmiştir. Buna göre, temel alan bilimsel hesaplama, seçmeli alanlar da, optimizasyon, dinamik sistemler, hesaplamalı akışkanlar mekaniği ve sonlu elemanlar konularından oluşmuştur. Kasım ayında yapılan ilk doktora yeterlilik sınavına dört öğrenci katılmış ve bu öğrenciler sınavı başarıyla geçmişlerdir.

2005-2006 öğretim yılında UME Bilimsel Hesaplama programına basvuran 39 öğrenciden 20'si kabul edilmiş, ancak bunlardan 13'ü programa kayıt yaptırmıştır. Yüksek lisans programına kabul edilen öğrencilerin LES puanları ortalaması 69.65, CGPA ortalaması 3.08/4.00, Doktora programına kabul edilen öğrencilerin LES puanları ortalaması ise 64.25, CGPA ortalaması 3.23/4.00'dir.

2005-2006 öğretim yılında programa kabul edilen öğrencilerin %55'i lisans derecesini ODTÜ'den almış ve bunların da %60'ı Matematik Bölümü mezunlarıdır. Diğer öğrencilerin, lisans derecelerini aldıkları üniversite ve bölümleri aşağıdaki gibidir.

Üniversiteler:

- Hacettepe Üniversitesi, Gazi Üniversitesi, Çankaya Üniversitesi,Ankara Üniversitesi ve Grove City College.

Bölümler:

- Matematik, Fizik, Bilgisayar Mühendisliği, Elektrik-Elektronik Mühendisliği ve Endüstri Mühendisliği.

Bilimsel Hesaplama Anabilim dalında tezli yüksek lisans ve doktora programları mevcuttur. Bu yıl tezli yüksek lisans programından beş öğrenci mezun olmuştur. **Ek 5'**de yüksek lisans tezlerinin başlıklarını bulabilirsiniz. (http://www.iam.metu.edu.tr/body1.php?PageId=160500)

KONFERANS KATILIMLARI

- **Ö. Uğur,** "Numerical Method for Optimizing Stirrer Configurations", The Sixth European Conference on Numerical Mathematics and Advanced Applications, ENUMATH 2005, Santiago de Compostela, Spain, July 18-22, 2005.

- **S.Özöğür**, "Machines Learning, Support Vector Machines, and Large Scale Optimization" Bayreuth University, Germany, March 16-18, 2005.

- **G. W. Weber, B. Karasözen, "**On Semi-Infinite Optimization of Anticipatory Systems and Their Modern Applications", 8. SIAM Conference on Optimization Stockholm, Sweden, May 15-19, 2005.

- **G. W. Weber,** "Challenges in the Optimization of Bio-Systems in Nature, Industry and Society, EURO Mini Conference "Optimization in the Industry", Pécs, Hungary, June 29 - July 1, 2005.

- **G. W. Weber,** "Discrete Tomography: a Joint Contribution by Optimization, Equivariance Analysis and Learning" CASYS'05, "Seventh International Conference on Computing Anticipatory Systems", Liege, Belgium, August 8-13, 2005.

- **G. W. Weber**, "An Anticipatory Extension of Malthusian Model", CASYS'05, "Seventh International Conference on Computing Anticipatory Systems", Liege, Belgium, August 8-13, 2005.

- **G. W. Weber,** "Challenges in the Optimization of Bio-Systems", International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

- **G. W. Weber,** "Anticipatory Extensions of Malthusian Model" , International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

- **H. Öktem, Ö. Uğur, S. Gürol,** "Ulusal İklim Bilimleri Kollokyumu", Mersin, 6-8 Nisan 2005.

YURT DIŞI İLİŞKİLER

- **Ö. Uğur**, Technical University of Kaiserslautern and Fraunhofer ITWM, Almanya, 1 Haziran-30 Temmuz 2005.

- **Ö. Uğur**, Department of Numerical Methods in Mechanical Engineering, Darmstadt University of Technology, Almanya, 1-30 Agustos 2005.

- **B. Karasözen**, Department of Numerical Methods in Mechanical Engineering, Darmstadt University of Technology, Almanya, 1 Şubat – 1 Mart 2005.

- **B. Karasözen**, Department of Numerical Methods in Mechanical Engineering, Darmstadt University of Technology, Almanya, 1-30 Haziran 2005.

- **B. Karasözen**, Department of Chemical Engineering, University of Carnegie Mellon, Amerika, 1-15 Ağustos 2005.

- **Z. Alpaslan**, Universität der Bundeswehr München, Almanya, 22 Haziran-19 Temmuz 2005.

YÜRÜTÜCÜLÜĞÜ YAPILAN PROJELER

DEVAM EDEN PROJELER

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

Projenin Adı: Nükleer Füzyon Reaktör Problemlerinin Sınır Elemanları ve Sonlu Elamanlar Yöntemleri ile Çözümü
Yürütücüsü: M. Tezer
Araştırmacıları: A İ. Neslitürk (İzmir Yüksek Teknoloji Enstitüsü), S. Han Aydın (UME doktora öğrencisi), S. Gümgüm (UME doktora öğrencisi, İzmir Ekonomi Üniversitesinde Öğretim Görevlisi)
Süresi: 1 Kasım 2005 – 1 Kasım 2007

Projenin Adı: Modeling Multistationary Processes by Using Hybrid System Formulation: A study with priority on functional genomics (TÜBİTAK kariyer projesi)
Yürütücüsü: Hakan Öktem
Araştırmacıları: D. Akçay, Ö. Hakanoğlu
Süresi: Haziran 2005 –Haziran 2010

Projenin Adı: Sürekli Optimizasyon Yöntemleri ve Uygulamaları (TÜBİTAK Bütünleşik Doktora Programı projesi)
Yürütücüsü: B. Karasözen
Araştırmacıları: G. W. Weber, T. Ergenç, Y. Uludağ
Süresi: 2005-2008

TAMAMLANAN PROJELER

Projenin Adı: Volkswagen Vakfı destekli "Stirrer Optimization" projesi
Yürütücüsü: M. Schaefer (Darmstadt Teknik Üniversitesi Makina Mühendisliği)
Araştırmacıları: B. Karasözen, Ö. Uğur, K. Yapıcı (Kimya Mühendisliği), Y. Uludağ (Kimya Mühendisliği)
Süresi: Nisan 2003 – Nisan 2005

PROGRAM 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: 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

DÜZENLENEN TOPLANTILAR

- 9. İleri Mühendislik konularında Türk-Alman Yaz Akademisi, Kuşadası, İzmir, 28 Ağustos - 3 Eylül 2005.

- HIBIT, "International Symposium on Health Informatics and Bioinformatics", Antalya, 10-12 Kasım 2005.

HALKA AÇIK KISA SÜRELİ KURSLAR/SEMİNERLER

- **Oliver Stein** (Aachen University), "Lectures on modern concepts in semi-infinite optimization", 23 – 30 Eylül 2005.

- **Adil Bagirov** (University of Ballarat), "Lectures on Derivative-free nonsmooth optimization and its Applications", 2-14 Ekim 2005.

- **Alexander Rubinov** (University of Ballarat), "Abstract Convexity with Applications to Global Optimization", 2-5 Ekim 2005.

- **Phlippe Toint** (University of Namur), "Lectures on trust region method and optimization partially separable functions", 6-13 Kasım 2005.

DÜZENLENEN ÇALIŞTAYLAR/SEMİNER

- **G. W. Weber,** "Workshop on Sustainable Living in Rural Areas of Turkey", Ankara, 7-21 Mart 2005.

DERGİ EDİTÖRLÜKLERİ

- **G. W. Weber**, Member of Editorial Board of Journal of Computational Technologies.

- **B. Karasözen, M. Pinar, T. Terlaky and G.-W. Weber**, Advances in Continuous Optimization, special issue of European Journal of Operational Research 169, 3 (2006).

- **B. Karasözen, A. Rubinov, G.-W. Weber, J. Teghem,** Optimization in Data Mining, special issue of European Journal of Operational Research (2005-2006).

- **M. Dür, B. Karasözen, T. Terlaky and G.-W. Weber, J. Teghem**, Challenges of Continuous Optimizatiom in Theory and Applications, special issue of European Journal of Operational Research (2005-2006).

YURT DIŞI YAYINLAR

- **Öktem, H.**, "A Survey on Piecewise-linear Models of Regulatory Dynamical Systems Nonlinear Analysis", Theory, Methods and Applications, 63 (3), 336-349, 2005.

- **Karasözen, B., Tsybulin, V.G.,** "Cosymmetry Preserving Finite-Difference Methods for Convection Equations in a Porous Medium", Applied Numerical Mathematics, 55 (1), 69-82, 2005.

- **Karasözen, B., Tsybulin,V.G.,** "Mimetic Discretization of two Dimensional Darcy Convection", Computer Physics Communications, 167, 207-213, 2005.

- **Akhmet, M.U.,** "On the Smoothness of Solutions of Impulsive Autonomous Systems Nonlinear Analysis", Theory, Methods and Applications, 60 (2), 311-324, 2005.

- **Schäfer, M., Karasözen, B., Uludağ, Y., Yapıcı, K., Uğur, Ö.**, "Numerical Method for Optimizing Stirrer Configurations", Computers and Chemical Engineering, 30 (2), 183-190, 2005.

- **Akalın, E., Akhmet, M.U.,** "The Principles of B-smooth Discontinuous Flows" Computers and Mathematics with Applications, 49 (7-8), 981-995, 2005.

- **Akhmet, M.U.,** "Perturbations and Hopf Bifurcation of the Planar Discontinuous Dynamical System Nonlinear Analysis", Theory, Methods and Applications, 60 (1), 163-178, 2005.

- **Akhmet, M.U., Kirane, M., Tleubergenova, M.A., Weber, G.W.,** "Control and Optimal Response Problems for Quasilinear Impulsive Integrodifferential Equations", European Journal of Operational Research, 169 (3), 1128-1147, 2005.

- **Akhmet, M.U., Gebert, J., Öktem, H., Pickl S. W., and Weber**, **G.-W., "**An Improved Algorithm for Analytical Modeling and Anticipation of Gene Expression Patterns", Journal of Computational Technologies 10, 4 3-20, 2005.

YURT DIŞI TEBLİĞLER

- **M.Tezer–Sezgin, S. H. Aydın,** "Numerical Solution of MHD flow problems using BEM", Boundary Elements XXVII, WIT Press, USA, 458, 2005.

- **F.B. Yılmaz, H. Öktem and G.-W. Weber**, "Mathematical modeling and approximation of gene expression patterns and gene networks", in: Operations Research Proceedings, at the occasion of International Conference on Operations Research, Tilburg, The Netherlands, September 2004, 280-287, 2005.

- **M.U. Akhmet, H. Öktem, S.W. Pickl and G.-W. Weber**, "An Anticipatory Extension of Malthusian Model", to appear in the proceedings of CASYS'05, Seventh International Conference on Computing Anticipatory Systems, Belgium, August, 2005 *(Best Paper Award)*.

- **M. Taştan, S.W. Pickl and G.-W. Weber**, "Mathematical Modeling and Stability Analysis of Gene-Expression Patterns in an Extended Space and with Runge-Kutta Discretization", Germany, September 2005.

YURT İÇİ TEBLİĞLER

- **S. Özöğür, A. Sağdıçoğlu Celep, B. Karasözen, N.Yıldırım and G.-W. Weber**, "Dynamical Modelling of Enzymatic Reactions, Simulation and Parameter Estimation with Genetic Algorithms", in: HIBIT - Proceedings of International Symposium on Health Informatics and Bioinformatics, Turkey '05, Antalya, November 2005, 78-84.

- **M. Taştan, T. Ergenc, S.W. Pickl and G.-W. Weber**, "Stability Analysis of Gene Expression Patterns by Dynamical Systems and a Combinatorial Algorithm", in: HIBIT - Proceedings of International Symposium on Health Informatics and Bioinformatics, Turkey '05, Antalya, November 2005, 67-75.

YURT DIŞI SUNUMLAR

- **G. W. Weber,** "Challenges in the Optimization of Bio-Systems" Common Workshop of GOR (German OR Society) Working Groups, "OR im Umweltschutz" und "Optimierung von Biosystemen": "Environmental Management und komplexe Biosysteme", University of Siegen, Germany, March 10-11, 2005.

- **G. W. Weber**, "Anticipation and Optimization of Gene Expression Patterns" PASCAL Tutorial and Workshop "Machine Learning, Support Vector Machines, and Large-Scale Optimization", Wissenschaftszentrum Schloss Thurau, Germany, March 16-18, 2005.

- **A. Tezel, G. W. Weber, B. Karasözen, T. Ergenç,** On Semi-Infinite Optimization of Anticipatory Systems and Their Modern Applications, 8. SIAM Conference on Optimization Stockholm , Sweden, 15-19 Mayıs, 2005.

- **G. W. Weber,** "Challenges in the Optimization of Bio-Systems", "Workshop on Algorithmic Techniques for Data Mining", ORT Braude College, Karmiel, Israel, May 30, 2005.

- **S. W. Pick, G. W. Weber**, "On Optimal Control of Heating Processes, On Semi-Infinite Optimization of Anticipatory Systems and Their Modern Applications", 8. SIAM Conference on Optimization Stockholm , Sweden, 15-19 Mayıs, 2005.

- **G. W. Weber**, "Challenges in the Optimization of Bio-Systems in Nature, Industry and Society, EURO Mini Conference "Optimization in the Industry", Pécs, Hungary, June 29 - July 1, 2005.

- **G. W. Weber**, "Challenges in the Optimization of Bio-Systems, SSIP 2005 "13th Summer School on Image Processing", Szeged, Hungary, June 30 – July 8, 2005.

- **Ö. Uğur,** Numerical Method for Optimizing Stirrer Configurations, The Sixth European Conference on Numerics, Mathematics and Advanced Applications, ENUMATH 2005, Santiago de Compostela, Spain; 18--22 July 2005.
- **G. W. Weber, A. Kuba, Ö.Yaşar,** "Discrete Tomography: a Joint Contribution by Optimization, Equivariance Analysis and Learning" CASYS'05, "Seventh International Conference on Computing Anticipatory Systems", Liege, Belgium, August 8-13, 2005.

- **G. W. Weber, M. Akhmet, H. Öktem, Z. Alparslan, A.Tezel, S.W. Pickl** , "An Anticipatory Extension of Malthusian Model", CASYS'05, "Seventh International Conference on Computing Anticipatory Systems", Liege, Belgium, August 8-13, 2005.

- **G. W. Weber, M. Akhmet, S.W. Pickl,** "Challenges in the Optimization of Bio-Systems", International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

- **G. W. Weber, M. Akhmet, H. Öktem, S.W. Pickl**, "Anticipatory Extensions of Malthusian Model" , International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

- **G. W. Weber, A. Tezel,** "Generalized Semi-Infinite Optimization and Anticipatory Systems", International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

YURT İÇİ SUNUMLAR

- **S. Gürol, H. Öktem, T. Özalp, B. Karasözen,** Statistical Learning and Optimization Methods For Improving the Efficiency in Landscape Image Clustering and Classification Problems, ISPRS Workshop on Spatial/Spatio-Temporal Data Mining(SDM) and Learning, METU, Ankara, November 24-25, 2005.

- **G.-W. Weber, A. Kuba, Ö.Yaşar, E. Dağlı, O. Özgür,** "Discrete Tomography: a Joint Contribution by Optimization, Equivariance Analysis and Learning" ISPRS 2005 "Spatial Data Mining Workshop", METU, Ankara, November 24-25, 2005.

RAPORLAR

- **G. Waescher and G.-W. Weber,** Was hat Sie eigentlich nach Ankara ,,verschlagen" Herr Weber, interview by Gerhard Waecher, president of German Operations Research Society (GOR), OR-News 23, 71-74, Maerz 2005.

- **G.-W. Weber,** Wissenschaftlicher Austausch und Zukunftsimpulse aus dem Herzen Europas - Bericht ueber die 17. EURO Mini-Konferenz "Continuous Optimization in the Industry", Pécs, Ungarn, OR-News 25 (German OR Society) 69-71, 29, Hungary, Juni - 1. Juli 2005.

- **G.-W. Weber,** Book Review -- Bernt Oksendal and Agnes Sulem (2005), Applied Stochastic Control of Jump Diffusions, ISBN 3-540-14023-9, Math. Meth. Oper. Res. 62, 2, 345-346, Germany, 2005.

DOSAP PROGRAMI

- **Pakize Taylan** (Dicle Üniversitesi, Matematik Bölümü), Finansal Piyasalarda Matematiksel Optimizasyon Tekniklerinin Kullanımı (1 Ekim 2005- 30 Eylül 2006)

- **Rengin Ak** (Yüzüncü Yıl Üniversitesi, Iktisat Bölümü), Finansal Piyasalarda Ve Kredi Riskinin Optimizasyon Yöntemlerinin Kullanılması (1 Ekim 2005- 30 Eylül 2006)

MİSAFİR ÖĞRETİM ÜYELERİ

- **Dr. Dorien DeTombe**, University of Amsterdam, Chair of International and EURO Working Group on Complex Societal Problems 6-23 Mart, 2005.

- **V. Tkachenko,** Institute of Mathematics National Academy of sciences, Kiev, Ukraine, Mart-Mayıs 2005.

- **V. G. Tsybulin**, Rostov State University, 25 Nisan -25 Mayıs 2005.

- **Oliver Stein,** Aachen Üniversity, 23 – 30 Eylül 2005.

- **Adil Bagirov**, University of Ballarat, 2-14 Ekim 2005.

- **Alexander Rubinov**, University of Ballarat, 2-5 Ekim 2005.
- **Phlippe Toint**, University of Namur, 6-13 Kasım 2005.

ÖDÜLLER

- **Fatma Bilge Yılmaz** (Bilimsel Hesaplama) Yüksek Lisans Tez Ödülü.
- **Selime Gürol** (Bilimsel Hesaplama) Yüksek Lisans Ders Performans Ödülü.

ARAŞTIRMA GRUPLARI

HESAPLAMALI BİYOLOJİ VE TIP ARAŞTIRMA GRUBU

Araştırma Grubumuzda yer alan temel konuları: 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 kontrolü şeklinde sıralayabiliriz.
Grubun web sitesi, http://www.iam.metu.edu.tr/research/groups/compbio/index.html adresindedir.

Araştırma grubumuz 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 temsilcimiz bulunmaktadır.

Çalışma grubu tarafından düzenlenen haftalık seminerde toplam 37 sunum yapılmış, gruptaki öretim üyesi ve öğrenci sayısı 64'dir. Grubun 2005 yılı etkinlikleriyle ilgili özet bilgiler aşağıda verilmiştir:

- Üniversitedeki Biyotıp Bilim ve Teknolojileri YUUP grubuyla ve bu çerçevede GATA'yla (Gülhane askeri Tıp Akademisi) ortak çalışmalar sürdürülmüştür.
- Enformatik Enstitüsü, Bilgisayar Mühendisliği ve Biyoloji Bölümleriyle birlikte Antalya'da 10-12 Kasım 2005 tarihlerinde, HIBIT, "International Symposium on Health Informatics and Bioinformatics" konferansı düzenlenmiştir.
- Max-Planck Enstitüsü Schangai ile birlikte, 10-12 Eylül 2006'da düzenlenecek, Workshop on Networks in Computational Biology'nın hazırlıkları yapılmıştır.

OPTİMİZASYON TEORİSİ ARAŞTIRMA GRUBU

Enstitümüz bünyesinde kurulan **Optimizasyon Araştırma Grubu**, global, yarı-sonsuz değişkenli, türevsiz ve düzgün olmayan optimizasyon konularında çalışmalar yapmaktadır. Grubun 2005 yılı etkinlikleriyle ilgili özet bilgiler aşağıda verilmiştir:

- Darmstadt Teknik Üniversiteyle birlikte yürütülen 'Stirrer Optimization' projesi sonuçlandırılmıştır.
- Avrupa Yöneylem Dernekleri (EURO)'nin bir alt kuruluşu olan **EUROPT'un** (EURO Working Group on Continous Optimization) eşbaşkanlığını enstitümüz öğretim üyelerinden G. W. Weber yürütmektedir ve bu kuruluşun web sayfasına Enstitümüz ev sahipliği yapmaktadır. Bu grup tarafından 29 Haziran – 1 Temmuz tarihlerinde, Macaristan, Pecs'de "7th EURO Mini Conference Optimization in the Industry", 11-15 Temmuz 2005 tarihlerinde, Hawai'de IFORS 2005 toplantısında bir oturum düzenlenmiştir. Enstitü'nün girişimiyle EURO içinde 'Operational Research for Development' çalışma grubu kurulmuş, EUROPT üye sayısı 460'a ulaşmış, Enstitü içinde EURO çalışma gruplarından olan YORC (Young People People for Operational Research in Developing Countries) oluşturulmuştur.
- "Sürekli Optimizasyon Yöntemleri ve Uygulamaları" TÜBİTAK Bütünleşik Doktora Programı projesi çerçevesinde, Eylül-Kasım 2005'de O. Stein, A. Bagirov, A. Rubinov ve P. Toint seminerler vermiş ve çesitli konuşmalar yapmışlardır.

Grubun web sitesi, http://www.iam.metu.edu.tr/research adresinde görülebilinir.

DİNAMİK SİSTEMLER ARAŞTIRMA GRUBU

Enstitümüz bünyesinde oluşan **"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.

Misafir öğretim üyelerinden V. G. Tsybulin ve V. Tkachenko tarafından üç seminer verilmiştir. Öğrenciler ve öğretim üyeleri tarafından grup seminerlerinde yapılan sunumlarla çalışmalar yürütülmektedir.

Grubun web sitesi, http://www.iam.metu.edu.tr/research adresinde görülebilinir.

TERS PROBLEMLER ARAŞTIRMA GRUBU

Grubun 2005 yılı çalışmaları, diğer grupların çalışmalarına ve projelerine destek şeklinde, ortaklaşa yürütülmüş olup, grup üye sayısı 35'dir.

Grubun web sitesi, http://www.iam.metu.edu.tr/research adresinde görülebilinir.

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.

Grubun web sitesi, http://www.iam.metu.edu.tr/research adresinde görülebilinir.

FİNANSAL MATEMATİK PROGRAMI

Finansal Matematik programında 2005-2006 I. döneminde Doktora programı başlatılmış ve doktora yeterlilik konuları, Olasılık Teorisi, Stokastik Prosesler, Finansal Türevler, Finansal Ekonomi olarak belirlenmiştir. Kasım ayında yapılan ilk doktora yeterlilik sınavına giren 1 öğrenci başarılı olmuştur.

2005 öğretim yılında Finansal Matematik programına başvuran 79 öğrenciden 39'u kabul edilmiş, ancak bunlardan 23'ü kayıt yaptırmıştır. Hayat Sigortası Opsiyonuna ise başvuran 9 öğrenciden 7'si kabul edilmiş, ancak bunlardan 4'ü kayıt yaptırmıştır. Finansal Matematik Yüksek lisans programına kabul edilen öğrencilerin LES puanları ortalaması 67.95, CGPA ortalaması 3.36/4.00, Doktora programına kabul edilen öğrencilerin LES puanları ortalaması 66.55, CGPA ortalaması 2.98/4.00 iken Hayat sigortası opsiyonunda Programa kabul edilen öğrencilerin LES puanları ortalaması 66.7, CGPA ortalaması 3.03/4.00'tür.

2005 öğretim yılında Finansal Matematik programına kabul edilen öğrencilerin %69'u lisans derecesini ODTÜ 'den almış ve %38'i Matematik Bölümü mezunlarıdır. Diğer taraftan kabul edilen öğrencilerin, lisans derecelerini aldıkları üniversite ve bölümler aşağıda belirtilmiştir:

Üniversiteler:
- Bilkent Üniversitesi, Hacettepe Üniversitesi, Ankara Üniversitesi, Başkent Üniversitesi, Dokuz Eylül Üniversitesi ve Ege Üniversitesi,.

Bölümler:
- Matematik, İstatistik, İşletme, İktisat, Fizik ve Bilgisayar Mühendisliği.

2005 öğretim yılında Hayat Sigortası opsiyonuna kabul edilen öğrencilerin %86'sı lisans derecesini ODTÜ'den almıştır. Diğer öğrencilerin lisans derecelerini aldıkları üniversite ve bölümler aşağıdaki gibidir.

Üniversiteler:
- Ege Üniversitesi.

Bölümler:
- İktisat, İstatistik.

Finansal Matematik Anabilim dalında doktora ve tezli/tezsiz yüksek lisans programları mevcut bulunmakta, Hayat Sigortası Opsiyonunda ise sadece tezsiz yüksek lisans programı yer almaktadır. Finansal Matematik Anabilim dalımızda doktora ve tezli/tezsiz yüksek lisans programları sürdürülmektedir. Finansal Matematik tezli yüksek lisans programından 6, tezsiz programdan 7, Hayat Sigortası Opsiyonunda ise 8 öğrenci mezun olmuştur. **(Ek 5)**

KONFERANS KATILIMLARI:

- **Kasırga Yıldırak, Ayşegül İşcanoğlu** "Credit Scoring Methods", First International Conference on Business, Management and Economics" Yaşar Üniversitesi, Çeşme, 16-19 Haziran 2005.

- **Kasırga Yıldırak, İrem Yıldırım, Zehra Ekşi** "Alternative Risk Measures and Extreme Value Theory in Finance: Implementation on ISE 100 Index" First International Conference on Business, Management and Economics" Yaşar Üniversitesi, Çeşme, 16-19 Haziran 2005.

ULUSLARARASI PROTOKOLLER:

- UME Finansal Matematik Programı, **Yunanistan Aegean Üniversitesi** Statistik ve Aktuarya Bilimleri Bölümü ile müşterek araştırmalar yürütmek ve ortak doktora öğrencileri yetiştirmek üzere bir protokol imzalanmıştır. Bu protokolün tam metni www.iam.metu.edu.tr/intagree adresinde bulunabilir.
- **Fransa La Rochelle Üniversitesi** ile **UME** arasında, öğretim üyesi ve öğrenci değişimiyle Finans Matematiği alanında elde edilmiş olan deneyimlerin karşılıklı aktarılması ve Avrupa araştırma projelerine müşterek katılım amacıyla bir anlaşma yapılmıştır. Bu kapsamda 2004-2005 II. döneminde N.Privault, üniversitemizi ziyaret etmiştir. Bu işbirliği önümüzdeki dönemde de devam edecektir.

HALKA AÇIK KISA SÜRELİ KURSLAR/SEMİNERLER:

Finansal Matematik programının halka, özellikle de paydaşlara açık kısa süreli kursları kapsamında 2005 yılının Haziran ayında Hayri Körezlioğlu ve Kasırga Yıldırak tarafından 3 gün süreli **"Matlab yardımı ile Finansal Risk Hesabı"** başlıklı T.C. Merkez Bankası, Hazine Müsteşarlığı, Vadeli İşlemler Borsası, BDDK, bankalar ve diğer üniversiteden katılımcıların izlediği çalıştay düzenlenmiştir.

2005-2006 eğitim dönemi Eylül ayında Prof. Dr. Hayri Körezlioğlu, tarafından "Bilkent University Seminars on Financial Mathematics Academic Year 2005-2006" kapsamında "Introduction to Financial Mathematics" başlıklı üç eğitim semineri vermiştir.

2005 yılında yabancı katılımcılar tarafından **5 seminer** gerçekleşmiştir. Bu seminerlerin içeriğine www.iam.metu.edu.tr/seminars adresinden ulaşılabilinir.

DOSAP PROGRAMI

- **Ş. Kasırga Yıldırak** (Trakya Üniversitesi, İktisat Bölümü), Finansal Kurumlar İçin Kredi Değerlendirmesi ve Risk Ölçümleri (15 Eylül 2005- 15 Eylül 2007).

ARAŞTIRMA GRUPLARI

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)

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. Grubun 2005 yılı etkinlikleri aşağıda verilmiştir:

- Yüksek lisans öğrencileri tarafından tez konularıyla ilgili toplam 30 sunum yapılmıştır.
- 11-12 Mayıs tarihlerinde 'Mathematical Awareness' etkinlikleri çerçevesinde Matematik ve Uzay' konusunda çeşitli sunumlar ve video gösterisi yapılmıştır.

Misafir konuşmacılar:

- E. Özsoy, "Simple Ecosystem Models", METU, Institute of Marine Sciences, 7 Ocak 2005.
- O. Kaynak, "Mechatronics in 21st Century", Boğazici University, Electrical and Electronics Department, 11 Mart, 2005.

Grup hakkında ayrıntılı bilgiye www.siam.metu.edu.tr adresinden ulaşlabilinir.

2005 UME BÜTÇESİ

Enstitümüzün finansal kaynakları; Katma Bütçe, Ö.S.H.B. Saymanlığı, BAP ve ÖYP'den aldığı paylardan oluşmaktadır. Katma Bütçe ve Ö.S.H.B. Saymanlığı'ndan ayrılan pay kısıtlı olduğundan enstitünün ihtiyaçları BAP projelerinden karşılanmıştır. Enstitümüz Ö.S.H.B. Saymanlığı payının hemen hemen tamamı Reuters üyelik ücreti ve öğrenci asistan ücretli olarak kullanılmıştır. ÖYP Bütçesi daha çok bilgisayar öğrenci laboratuarının işler hale gelmesi için gerekli eksikliklerin giderilmesi ve ofislerde masa, dolap, bilgisayar gibi ofis gereksinimlerini karşılamak üzere kullanılmıştır. Enstitümüze ayrılan paylar ve harcanan miktar aşağıda verilmiştir.

	Ayrılan Kaynak (YTL)	**Harcanan (YTL)**
Öğrenci S. Hizmetler B.Saymanlığı Katma Bütçe	**5.780**	**5.780**
200 (Seyahat)	**1.420**	**-**
400 (Malzeme)	**1.420**	**1.420**
Toplam :	**8.620**	**7.200**

	Ayrılan Kaynak (YTL)	**Harcanan (YTL)**
BAP		
1 Adet (DAP)	**8.000**	**2.000**
11 Adet Tez Projesi	**31.002**	**31.002**
Toplam:	**39.002**	**33.002**
ÖYP (6 öğrenci)	**95.000**	**54.402**
Ek ödenekle birlikte		

Bunların yanı sıra 2004 yılında DPT desteği alan Kriptoloji Araştırma laboratuarı altyapı projesinin bu yıl ayrılan payının hemen hemen tamamı öncelikle inşaata harcanmıştır.

EKLER

EK: 1
YAYINLAR VE IAM PREPRINT SERİSİ

YAYINLAR:

- **E. Saygı, Z. Saygı, M. Sönmez Turan, A. Doğanaksoy**, "Statistical Approach on the Number of SAC Satisfying Functions", BFCA'05, First Workshop on Boolean Functions: Cryptography and Applications, Rouen , France, 2005.

- **E.Çakçak, F. Özbudak**, "Number of Rational Places of Subfields of the Function Field of the Deligne-Lusztig Curve of Ree Type", Acta Arith. 120, no.1, 79-106, 2005.

- **Schäfer, M., Karasözen, B., Uludağ, Y., Yapıcı, K., Uğur, Ö.**, "Numerical Method for Optimizing Stirrer Configurations", Computers and Chemical Engineering, 30 (2), 183-190, 2005.

- **Akhmet, M.U., Kirane, M., Tleubergenova, M.A., Weber, G.W.,** "Control and Optimal Response Problems for Quasilinear Impulsive Integrodifferential Equations", European Journal of Operational Research, 169 (3), 1128-1147, 2005.

- **Akhmet, M.U., Gebert, J., Öktem, H., Pickl S. W., and Weber**, **G.-W., "**An Improved Algorithm for Analytical Modeling and Anticipation of Gene Expression Patterns", Journal of Computational Technologies 10, 4 3-20, 2005.

- **Öktem, H.**, "A Survey on Piecewise-linear Models of Regulatory Dynamical Systems Nonlinear Analysis, Theory", Methods and Applications, 63 (3), 336-349, 2005.

- **Karasözen, B., Tsybulin, V.G.,** "Cosymmetry Preserving Finite-Difference Methods for Convection Equations in a Porous Medium", Applied Numerical Mathematics, 55 (1), 69-82, 2005.

- **Karasözen, B., Tsybulin,V.G.,** "Mimetic Discretization of two Dimensional Darcy Convection", Computer Physics Communications, 167, 207-213, 2005.

- **Akhmet, M.U.,** "On the Smoothness of Solutions of Impulsive Autonomous Systems Nonlinear Analysis", Theory, Methods and Applications, 60 (2), 311-324, 2005.

- **Akalın, E., Akhmet, M.U.,** "The principles of B-smooth Discontinuous Flows" Computers and Mathematics with Applications, 49 (7-8), 981-995, 2005.

- **Akhmet, M.U.,** "Perturbations and Hopf Bifurcation of the Planar Discontinuous Dynamical System Nonlinear Analysis", Theory, Methods and Applications, 60 (1), 163-178, 2005.

YURT DIŞI TEBLİĞLER:

- **G. W. Weber, H. Öktem, M. Akhmedov, S. Pickl,** "An Anticipatory Extension of Malthusian Model", VII. International Conference on Computing Anticipatory Systems, Belgium, August 8-13, 2005 *(Best Paper Award)*.

- **M.Tezer–Sezgin, S. H. Aydın,** "Numerical Solution of MHD flow problems using BEM", Boundary Elements XXVII, WIT Press, USA, 458, 2005.

- **F.B. Yılmaz, H. Öktem and G.-W. Weber**, "Mathematical modeling and approximation of gene expression patterns and gene networks", in: Operations Research Proceedings, at the occasion of International Conference on Operations Research, Tilburg, The Netherlands, September 2004, 280-287, 2005.

- **M.U. Akhmet, H. Öktem, S.W. Pickl and G.-W. Weber**, "An anticipatory extension of Malthusian model", to appear in the proceedings of CASYS'05, Seventh International Conference on Computing Anticipatory Systems, Belgium, August, 2005.

- **M. Taştan, S.W. Pickl and G.-W. Weber**, "Mathematical Modeling and Stability Analysis of Gene-Expression Patterns in an Extended Space and with Runge-Kutta Discretization", Germany, September 2005.

YURT İÇİ TEBLİĞLER:

- **D. Toz, A. Doğanaksoy, M. Sönmez Turan**, "Statistical Analysis of Block Ciphers", 1. Ulusal Kriptoloji Sempozyumu, 56-66, 2005.

- **A. Doğanaksoy, B. G. Dündar, F. Göloğlu, Z. Saygı, F. Sulak, M. Uğuz**, "Constructions of Highly Nonlinear Balanced Boolean Functions", 1. Ulusal Kriptoloji Sempozyumu, 79-84, 2005.

- **F. Göloğlu, M. D. Yücel**, "Necessary Conditions on Balanced Boolean Functions with Maximum Nonlinearity", 1. Ulusal Kriptoloji Sempozyumu, 106-111, 2005.

- **A. Doğanaksoy, S. Sağdıçoğlu, Z. Saygı, M. Uğuz**, "An Interpretation of Sums of Walsh Spectrum Powers of Boolean Functions", 1. Ulusal Kriptoloji Sempozyumu, 112-116, 2005.

- **A. Doğanaksoy, E. Saygı**, **"**On The Quadratic Feedback Shift Registers**"**, 1. Ulusal Kriptoloji Sempozyumu, 127-133, 2005.

- **M. Cenk, F. Özbudak,** "Elliptic Eğri Kriptografi ve Aritmetiği", 1. Ulusal Kriptoloji Sempozyumu, 134-141, 2005.

- **F. Özbudak, Z. Saygı**, **"**Constructions of Systematic Authentication Codes**"**, 1. Ulusal Kriptoloji Sempozyumu, 143-148, 2005.

- **A. Doğanaksoy, F. Göloğlu**, **"**On Lempel-Ziv Complexity of Sequences**"**, 1. Ulusal Kriptoloji Sempozyumu, 149-155, 2005.

- **H.M. Yıldırım, E. Akyıldız**, **"**New Properties of IDEA ciphers Operations**"**, 1. Ulusal Kriptoloji Sempozyumu, 156-166, 2005.

- **O. Çetinkaya, A. Doğanaksoy,** "Electronic Voting Protocols Based on Blind Signatures", 1. Ulusal Kriptoloji Sempozyumu, 189-198, 2005.

- **S. Özöğür, A. Sağdıçoğlu Celep, B. Karasözen, N.Yıldırım, G.-W. Weber**, "Dynamical Modelling of Enzymatic Reactions, Simulation and Parameter Estimation with Genetic Algorithms", in: HIBIT - Proceedings of International Symposium on Health Informatics and Bioinformatics, Turkey '05, Antalya, November 2005, 78-84.

- **M. Taştan, T. Ergenc, S.W. Pickl and G.-W. Weber**, "Stability Analysis of Gene Expression Patterns by Dynamical Systems and a Combinatorial Algorithm", in: HIBIT - Proceedings of International Symposium on Health Informatics and Bioinformatics, Turkey '05, Antalya, November 2005, 67-75.

YURT DIŞI SUNUMLAR:

- **G. W. Weber,** "Challenges in the Optimization of Bio-Systems" Common Workshop of GOR (German OR Society) Working Groups, "OR im Umweltschutz" und "Optimierung von Biosystemen": "Environmental Management und komplexe Biosysteme", University of Siegen, Germany, March 10-11, 2005.

- **G. W. Weber**, "Anticipation and Optimization of Gene Expression Patterns" PASCAL Tutorial and Workshop "Machine Learning, Support Vector Machines, and Large-Scale Optimization", Wissenschaftszentrum Schloss Thurau, Germany, March 16-18, 2005.

- **A. Tezel, G. W. Weber, B. Karasözen, T. Ergenç,** On Semi-Infinite Optimization of Anticipatory Systems and Their Modern Applications, 8. SIAM Conference on Optimization Stockholm , Sweden, 15-19 Mayıs, 2005.

- **G. W. Weber,** "Challenges in the Optimization of Bio-Systems", "Workshop on Algorithmic Techniques for Data Mining", ORT Braude College, Karmiel, Israel, May 30, 2005.

- **S. W. Pick, G. W. Weber**, On Optimal Control of Heating Processes, On Semi-Infinite Optimization of Anticipatory Systems and Their Modern Applications, 8. SIAM Conference on Optimization Stockholm , Sweden, 15-19 Mayıs, 2005.

- **G. W. Weber**, "Challenges in the Optimization of Bio-Systems in Nature, Industry and Society, EURO Mini Conference "Optimization in the Industry", Pécs, Hungary, June 29 - July 1, 2005.

- **G. W. Weber**, "Challenges in the Optimization of Bio-Systems, SSIP 2005 "13th Summer School on Image Processing", Szeged, Hungary, June 30 – July 8, 2005.

- **Ö. Uğur,** Numerical Method for Optimizing Stirrer Configurations, The Sixth European Conference on Numerics, Mathematics and Advanced Applications, ENUMATH 2005, Santiago de Compostela, Spain; 18--22 July 2005.

- **G. W. Weber, A. Kuba, Ö.Yaşar,** "Discrete Tomography: a Joint Contribution by Optimization, Equivariance Analysis and Learning" CASYS'05, "Seventh International Conference on Computing Anticipatory Systems", Liege, Belgium, August 8-13, 2005.

- **G. W. Weber, Akhmet, H. Öktem, Z. Alparslan, A.Tezel, S.W. Pickl** , "An Anticipatory Extension of Malthusian Model", CASYS'05, "Seventh International Conference on Computing Anticipatory Systems", Liege, Belgium, August 8-13, 2005.

- **G. W. Weber, M. Akhmet, S.W. Pickl,** "Challenges in the Optimization of Bio-Systems", International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

- **G. W. Weber, M. Akhmet, H. Öktem, S.W. Pickl**, "Anticipatory Extensions of Malthusian Model" , International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

- **G. W. Weber, A. Tezel,** "Generalized Semi-Infinite Optimization and Anticipatory Systems", International Scientific Annual Conference "Operations Research 2005", Bremen, Germany, September 7-9, 2005.

YURT İÇİ SUNUMLAR

- **S. Gürol, H. Öktem, T. Özalp, B. Karasözen,** "Statistical Learning and Optimization Methods For Improving the Efficiency in Landscape Image Clustering and Classification Problems", ISPRS Workshop on Spatial/Spatio-Temporal Data Mining(SDM) and Learning, METU, Ankara, November 24-25, 2005.

- **G.-W. Weber, A. Kuba, Ö.Yaşar, E. Dağlı, O. Özgür,** "Discrete Tomography: a Joint Contribution by Optimization, Equivariance Analysis and Learning" ISPRS 2005 "Spatial Data Mining Workshop", METU, Ankara, November 24-25, 2005.

RAPOR:

- **G. Waescher and G.-W. Weber,** Was hat Sie eigentlich nach Ankara ,,verschlagen" Herr Weber, interview by Gerhard Waecher, president of German Operations Research Society (GOR), OR-News 23, 71-74, Maerz 2005.

- **G.-W. Weber,** Wissenschaftlicher Austausch und Zukunftsimpulse aus dem Herzen Europas - Bericht ueber die 17. EURO Mini-Konferenz "Continuous Optimization in the Industry", Pécs, Ungarn, OR-News 25 (German OR Society) 69-71, 29, Hungary, Juni - 1. Juli 2005.

- **G.-W. Weber,** Book Review -- Bernt Oksendal and Agnes Sulem (2005), Applied Stochastic Control of Jump Diffusions, ISBN 3-540-14023-9, Math. Meth. Oper. Res. 62, 2, 345-346, Germany, 2005.

IAM PREPRINT SERIES

No	Title – Abstract	Author	Date
29	Statistical approach on the number of SAC satisfying functions	E. Saygı, Z. Saygı, M. S. Turan, A. Doğanaksoy	02.28.2005
30	Dynamic Information Handling in Continuous Time Boolean Network Model of Gene Interactions	H. Öktem	02.28.2005
31	A Survey on Picewise-Linear Models of Regulatory Dynamical Systems	H. Öktem	03.08.2005
32	Anticipatory Extension of Malthusian Model	M. U. Akhmet , H. Öktem, S. W. Pickl, G.-W. Weber	03.18.2005
33	Numerical Solution of Magnetohydrodynamic Flow Problems Using Boundary Element Methood	M.Tezer-Sezgin, S.Han Aydın	04.05.2005
34	The dynamics of the systemic arterial pressure through impulsive differential equations	M.U.Akhmet, G.A.Bekmukhambetova, Y.Serinağaoğlu	04.05.2005
35	The Sturm-Liouville Operator on the Space of Functions with Discontinuity Conditions	M.U.Akhmet, Ö.Uğur	05.11.2005
36	On impulsive ratio-dependent predator-prey system with diffusion	M.U.Akhmet, M.Beklioglu, T.Ergenc, V.I.Tkachenko	05.30.2005
37	Modeling Gene Regulatory Networks with Piecewise Linear Differential Equations	J. Gebert, N. Radde, G.-W.Weber	06.27.2005
38	Exploiting Statistical Learning in Education	I. Gorgun and G. W. Weber	06.29.2005
39	Integral manifolds of differential equations with piecewice constant argument of generalized type	M.U.Akhmet	08.16.2005
40	Dynamical Modelling of Enzymatic Reactions, Simulation and Parameter Estimation with Genetic Algorithm	S.Özöğür, A. Gülçin S. Celep, B. Karasözen, N.Yıldırım, G.-W. Weber	08.16.2005
41	Challenges in the Optimization of Biosystems I: Parameter Estimation of Enzymatic Reactions with Genetic Algorithm	S.Özöğür, B. Karasözen, G.-W. Weber	08.16.2005
42	Challenges in the Optimization of Biosystems II: Mathematical Modeling and Stability Analysis of Gene-Expression Patterns in an Extended Space and with Runge-Kutta Discretization	M.Taştan, S.W. Pickl, G.-W. Weber	08.16.2005
43	Mathematical Modeling of Proximal Femur Geometry and Bone Mineral Density	M. Taştan, Ö. Çelik, G.-W. Weber, B. Karasözen, F. Korkusuz	08.16.2005
44	Modelling of Lipid Biosynthesis Pathways in Oil Palm	E.M.P Quek, G.-W. Weber, R. Sambanthamuthi	09.12.2005
45	Stability Analysis of Gene Expression Patterns by Dynamical Systems and a Combinatorial Algorithm	M. Taştan, T. Ergenç, S. W. Pickl, G.-W. Weber	09.20.2005
46	Statistical Learning and Optimization Methods for Improving the Efficiency in Landscape Image Clustering and Classification Problems	S. Gürol, H. Öktem, T. Özalp, B. Karasözen	12.09.2005
47	Representation of Zero Coupon Bond Prices in Terms of Two-Parameter Brownian Martingales	H.Körezlioğlu	12.21.2005

EK: 2
UME SEMİNERLERİ

Genel Seminerler

Credit Rating Models, Credit Risk Assessment and BASEL II	**Kasırga Yıldırak** (UME)	27 12 2005
Cyclical adjustment in stock markets and Hysteresis: the macroeconomic effects of technological progress	**Şaziye Gazioğlu** (Department of Economics)	20 12 2005
Pricing the Default Option of Inflation-Indexed Mortgages Using Explicit Finite Difference Method	**Işıl Erol** (Department of Economics)	13 12 2005
Security Issues of Network, Operating System and Application Layers -II	**Attila Ozgit** (Department of Computer Engineering)	29 11 2005
Security Issues of Network, Operating System and Application Layers -I	**Attila Ozgit** (Department of Computer Engineering)	22 11 2005
2007 ye doğru BASEL-II'ye geçişte Kredi Risk Yönetimi	**Kaan Aksel** (Pricewaterhouse Coopers)	15 11 2005
A Recursive Trust-Region Method for Multi-Scale Unconstrained Minimization	**Philippe L. Toint** (University of Namur)	08 11 2005
Elektrik Enerji Sektöründe Risk Yönetimi	**Osman Sevaioğlu** (Dept. of Electrical and Electronics Eng.)	18 10 2005
An Anticipatory Extension of Malthusian Model	**Gerhard W.Weber** (UME)	18 10 2005
Nonsmooth Optimization Approaches in Clustering and Supervised Data Classification Problems	**Adil M. Bagirov** (University of Ballarat Australia)	11 10 2005
Abstract Convexity with Applications to Global Optimization	**Alexander Rubinov** (University of Ballarat Australia)	04 10 2005
Solution methods in robust optimization	**Oliver Stein** (Aachen Univ. of Technology, Germany)	27 09 2005
Optimization of Re-injection in Geothermal Reservoirs	**Serhat Akın** (Dept. of Petrolcum–Natural Gas Eng.)	31 05 2005
Studying Behaviour	**Ewa Doğru** (Department of Biological Sciences)	24 05 2005
Applications of Braid Groups in Cryptography	**Ebru Keyman** (Department of Mathematics)	17 05 2005
Integrable Equations	**Konstyantyn Zheltukhyn** (Department of Mathematics)	10 05 2005
Families of steady states and dynamics in a system of parabolic equations (population kinetics model)	**Vyacheslav Tsybulin** (Rostov State University)	03 05 2005
Numerical Solution of Magnetohydrodynamic Flow Problems Using Boundary Element Method	**Selçuk Han Aydın** (UME)	26 04 2005
Monte Carlo methods and sensitivity analysis in markets with jumps	**Nicolas Privault** (Institute of Mathematics National Academy of Sciences, Kiev, Ukraine)	19 04 2005
Differentiation of some functionals of risk processes and optimal reserve allocation	**Stéphane Loisel** (Laboratoire SAF, Université Lyon 1, France)	12 04 2005
Some Classical One-Factor Interest Rate Models	**Yeliz Yolcu** (UME)	05 04 2005
On Complex Dynamical Systems & Fractals	**Figen Çilingir** (TOBB Ekonomi ve Teknoloji Üniv.)	29 03 2005
A Tour of Hybrid Approach to Modelling of Regulatory Dynamical Systems	**Hakan Oktem** (UME)	22 03 2005
The COMPRAM Approach: Handling Complex Problems in Real Life	**Dorien DeTombe** (University of Amsterdam, Chair of International and EURO Working Group on Complex Societal Problems)	15 03 2005
On stability in discrete population models with delayed-density dependence	**Viktor Tkachenko** (Institute of Mathematics National Academy of sciences, Kiev, Ukraine)	08 03 2005
On the representation of zero coupon bond prices in terms of random fields	**Hayri Körezlioğlu** (UME)	03 03 2005
A pedagogical walk through the non-perturbative objects, (solitons, instantons etc) in Quantum Field Theory	**Bayram Tekin** (Department of Physics)	04 01 2005

Grup Seminerleri

HESAPLAMALI BİYOLOJİ VE TIP ARAŞTIRMA GRUBU

A Database for Subcellular Localizations of Human Proteome based on P2SL -	**Biter Bilen** (Bilkent University, Department of Molecular Biology and Genetics)	30. 12. 2005
Resemblance of Turkish Human Population to the Populations of Balkans and Central Asia Based on Information Gained from Molecular Data -	**Ceren Berkman** (Department of Biology)	23. 12. 2005
YUUP:Gen-Pro: Bitkisel Genomik ve Proteomik Ulusal Mükemmeliyet Ağı -	**Mahinur Akkaya** (Department of Chemistry)	12. 12. 2005
Mitochondrial DNA (mtDNA) Sequence Analysis of Kangal Dogs in Turkey -	**Çiğdem Gökçek** (Department of Biology)	09. 12. 2005
Improving Sustainable Living in Rural Areas in Turkey -	**Ali Gökmen** (Department of Chemistry)	28.11.2005
Bioinformatics for fungal proteome-	**Volkan Yıldırım** (Department of Biological Sciences)	18.11.2005
Determination of Control Structure in Lipid Biosynthesis Pathways-	**Emily M. P. Quek** (Advanced Biotech. and Breeding Centre Malaysian Palm Oil Board, Malaysia)	07.11.2005
Some Remarks on Energy Management and Sustainable Development	**G. Wilhelm Weber** (UME)	21.10.2005
An Anticipatory Extension of Malthusian Model -	**G. Wilhelm Weber** (UME)	14.10. 2005
Discrete Tomography: A Joint Contribution by Optimization Equivariance Analysis and Learning	**G.Wilhelm Weber** (UME)	7.10. 2005
Discrete Tomography: A Joint Contribution by Optimization Equivariance Analysis and Learning -	**G.Wilhelm Weber** (UME)	30. 09. 2005
An Introduction to Semi-Infinite Optimization	**Aysun Tezel** (Dept. of Mathematics)	23. 09. 2005
Generalized Semi-Infinite Optimization and Anticipatory Systems	**G.Wilhelm Weber & Mesut Taştan** (UME)	16.09.2005
Protein-Destroying Nano-Compartments of Cells: Processive and Programmed Proteolytic Machineries and New Targets for Novel Drug Therapies -	**Semra Kocabıyık** (Department of Biology)	06.06.2005
Implicit motif distribution based hybrid computational kernel for sequence classification -	**Volkan Atalay** (Department of Biological Sciences)	03.06 .2005
Microarray Gene Expression Data ClusteringMicroarray Gene Expression Data Clustering -	**Biter Bilen** (Bilkent University, Department of Molecular Biology and Genetics)	27.05.2005
Studying Behaviour -	**Ewa Doğru** (Department of Biological Sciences)	24.05.2005
Optimization and Statistical Learning in Computational Biology and Medicine: Support Vector Machines and Their Modern Applications	**Süreyya Özöğür** (UME)	20.05.2005
Stability of Dynamical Systems: ◆A Constructive Approach -	**Mesut Taştan** (UME)	20.05.2005
Optimization, Dynamics and Optimal Control For CO2 Emission Reduction: The Technology Emission Means Model -	**Zeynep S. Alparslan** (UME)	20.05.2005
On Semi Infinite Optimization of Anticipatory Systems and Their Modern Applications -	**Aysun Tezel** (Department of Mathematics)	13.05.2005
Medical Informatics and a Case Study: Breast Diseases Cancer Research Database -	**Rıfat Hakan Otuz** (UME)	06.05.2005
Basic Introduction into the Nervous System, Hearing Physiology and Cochlear ImplantsBasic Introduction into the Nervous System, Hearing Physiology and Cochlear Implants -	**Burc Bassa** (Hacettepe University)	29.04.2005
Feedstock Optimization of In-vessel Food Waste Composting Systems for Inactivation of Pathogenetic Microorganisms -	**Deniz Çekmecelioğlu** (Department of Food Engineering)	21.04.2005

Bioinformatics Studies on Aspergillus fumigatus and Development of a PCR-Based Specific Detection Method by Random cDNA Cloning -	**Alper Söyler** (Dept. of Food Engineering)	15.04.2005
Strategies Towards Functional Analysis of Genes Associated with Roles in Wheat Stripe Rust Disease Resistance -	**Prof.Dr. Mahinur Akkaya** (Department of Chemistry)	08.04.2005
Prediction of Protein Subcellular Localization Based on Primary -	**Mert Özarar** (UME)	01.04.2005
MEETING with EXPERTS and ACTORS of Balaban project		21.03.2005
Balaban project expert meeting in Intelligent Class		21.03.2005
Mathematical Modelling of Enzymatic Reactions, Simulation and Parameter Estimation-	**Süreyya Özöğür** (UME)	04.03.2005
An introduction to methodologies on complex societal problems and Compram method -	**Dorien DeTombe** (University of Amsterdam, Chair of International and EURO Working Group on Complex Societal Problems)	07.03.2005
An introduction to Balaban project -	**Ali Gökmen** (Department of Chemistry)	7.03.2005
Engineering Nature & Engineering In Nature -	**Prof. Dr. Zümrüt Begüm Ögel**	24.02.2005
Applications of Semi-Infinite Programming /Generalized Semi-Infinite Programming and a new numerical method to solve SIP problems-	**Aysun Tezel** (Department of Mathematics)	6.01.2005

DİNAMİK SİSTEMLER GRUBU

Nonlinear Dynamics and Maple, MATLAB, Dynamic Solver	**V. G Tsybulin** (Mech.-Math. Faculty of Rostov State University , Department of Computational Mathematics and Mathematical Physics)	11.5.2005
Dynamics of One Dimensional Maps	**V. G Tsybulin** (Mech.-Math. Faculty of Rostov State University , Department of Computational Mathematics and Mathematical Physics)	27.4.2005
Population Dynamics and Impulsive Differential Equations	**Derya Altıntan** (UME)	13.4.2005
Continuous Dependence on Initial Value for Discontinuous Dynamical Systems	**Mehmet Turan** (Matematik Bölümü)	30.3.2005
On continuation of solutions of discontinuous dynamical systems	**Cemil Büyükadalı** (Matematik Bölümü)	16.3.2005
On predator-prey systems with diffusion and impulses	**Viktor Tkachenko** (Institute of Math., Kiev, Ukraine)	2.3.2005

HYBRİD SİSTEMLERİ ÇALIŞMA GRUBU

“Boolean Delay Equations for Abstraction of Hybrid Dynamical Systems”	**Hakan Öktem** (UME)	13 October 2005
“Fault Detection and Diagnosis in Nonlinear Dynamical Systems”	**Kemal Leblebicioğlu** (Dept.of El.Electronics Eng.)	06 October 2005

ÖĞRENCİ SEMİNERLERİ

Error Correcting Codes	**Özkan Boztaş**	24 12 2005
Modelling Portfolio Credit Risk	**Ayhan Yüksel**	24 12 2005
Optimal Reinsurance Strategies under Exponentially Distributed Claim Amounts	**Cengizhan Aksu**	21 06 2005
Insurer's Optimal Reinsurance Protections under Pareto Distributed Claim Amounts	**Gökhan Yılmaz**	21 06 2005
On factoring n with the b-algorithm	**Tamer Ergun**	17 06 2005
Probabilistic Primality Tests	**Atilla Bektaş**	15 06 2005
Algebraic Cryptanalysis of Stream Ciphers	**Burçin Erocal**	25 05 2005
Social Security Privization: Experiences Abroad	**Hacer Aydoğdu**	25 05 2005
Algebraic Cryptanalysis of Stream Ciphers	**Burçin Erocal**	25 05 2005
Social Security Privization: Experiences Abroad	**Hacer Aydoğdu**	25 05 2005
Enron Case	**Ayşe Kısacık**	18 05 2005
Too big to fail? Long-term Capital Management and the Federal Reserve	**Ebru Elif Gökçek**	18 05 2005
The Fall of MGRM	**Fatma Gaye Başaran**	18 05 2005
Simple Construction of the Efficient Frontier	**Efsun Kürüm**	11 05 2005
Seductive but Dangerous	**Aylin Akınlı**	11 05 2005
An investigation of the results of market liberalization in Turkey	**Utku Bora Geyikçi**	11 05 2005
Stochastic Pensions Plan	**Hale Taşkın**	04 05 2005
Insurer's Optimal Excess of Loss Strategy under a Static and Dynamic Situation	**Cengizhan Aksu**	27 04 2005
Static and Dynamic Optimal Reinsurance Strategy for a Non Proportional Treaty under a fixed Proportion	**Gökhan Yılmaz**	27 04 2005
Inference of switching networks by using a piecewise linear formulation	**Didem Akçay**	20 04 2005
Population Dynamics and Impulsive Differential Equations	**Derya Altıntan**	20 April 2005
Stability of Dynamical Systems:"A Constructive Approach"	**Mesut Taştan**	13 04 2005
The Technology Emissions Means Model	**Sırma Zeynep Alparslan**	13 04 2005
Modelling of Traffic Flow	**Nurşin Baş**	13 04 2005
Forecasting Stock Market Volatility : Evidence from Turkey	**Kadir Gürsoy**	13 01 2005
Authentication Codes from Higly Nonlinear Functions	**Mahir Ulutaş**	13 January 2005

EK: 3
ENSTİTÜMÜZÜ ZİYARET EDEN ÖĞRETİM ÜYELERİ

ENSTİTÜMÜZÜ ZİYARET EDEN ÖĞRETİM ÜYELERİ

Yurtiçi	Yurtdışı
E. Özsoy METU, Institute of Marine Sciences	**Oliver Stein** Aachen University
O. Kaynak Boğazici University	**Adil Bagirov** University of Ballarat
Çetin Kaya Koç İstanbul Ticaret Üniversitesi	**Alexander Rubinov** University of Ballarat
Ali Yazıcı ASELSAN Elektronik Sanayii ve Ticaret A.Ş.	**Phlippe Toint** University of Namur
Olay Salcan TÜBİTAK UEAKE	**Jurgen Lehn** Tecnische Universitat Darmstadt, Germany
Kaan Aksel Pricewaterhouse Coopers	**V. G. Tsybulin** Rostov State University
Figen Çilingir TOBB Ekonomi ve Teknoloji Üniv.	**Dorien DeTombe** University of Amsterdam, Holland
Biter Bilen Bilkent University, Department of Molecular Biology and Genetics	**V. Tkachenko** Institute of Mathematics National Academy of sciences, Kiev, Ukraine
Burc Bassa Hacettepe University	**Stéphane Loisel** Laboratoire SAF, Université Lyon 1, France
	Nicolas Privault Département de Mathématiques Université de La Rochelle **Institute of Mathematics National Academy of Sciences, Kiev, Ukraine)**
	Subhamoy Maitra Indian Statistical Institute, India
	Emily M. P. Quek Advanced Biotech. and Breeding Centre Malaysian Palm Oil Board, Malaysia

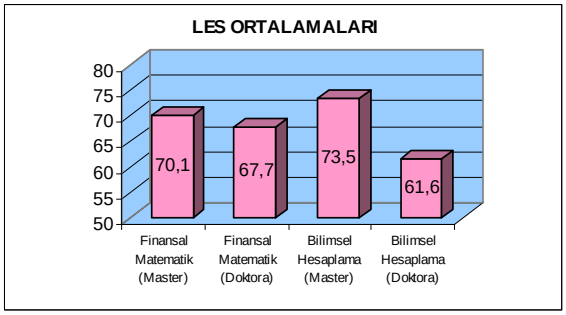
EK: 4
EĞİTİM VE ÖĞRENCİ İSTATİSTİKLERİ

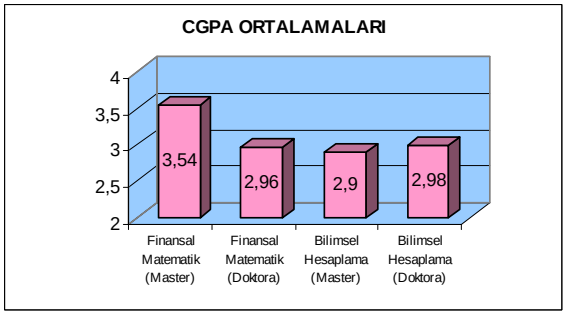
BAŞVURULAR

	2004-2005 II. Dönem			2005-2006 I. Dönem		
	BAŞVURU	KABUL	KAYIT	BAŞVURU	KABUL	KAYIT
Bilimsel Hesaplama	11	6	4	28	14	8
Finansal Matematik	22	9	9	57	30	19
Hayat Sigortası	-	-	-	9	7	4
Kriptografi	-	-	-	50	31	22
Toplam	33	15 (45%)	13 (39%)	144	82 (57%)	53 (37%)

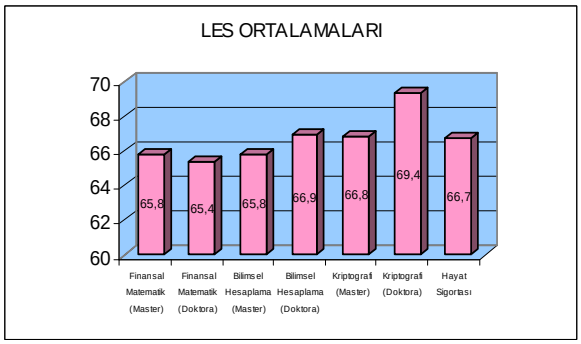
UME ÖĞRENCİLERİNİN LES VE CGPA ORTALAMALARI

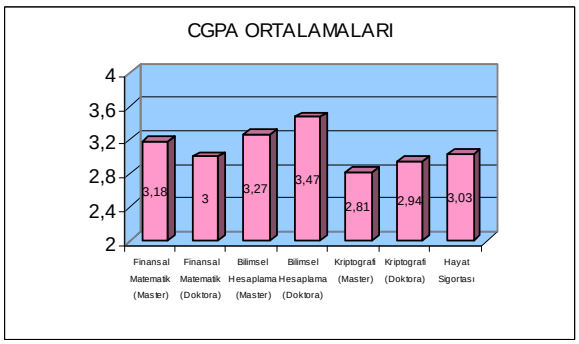
2004-2005 II. DÖNEM KABUL EDİLEN ÖĞRENCİLER



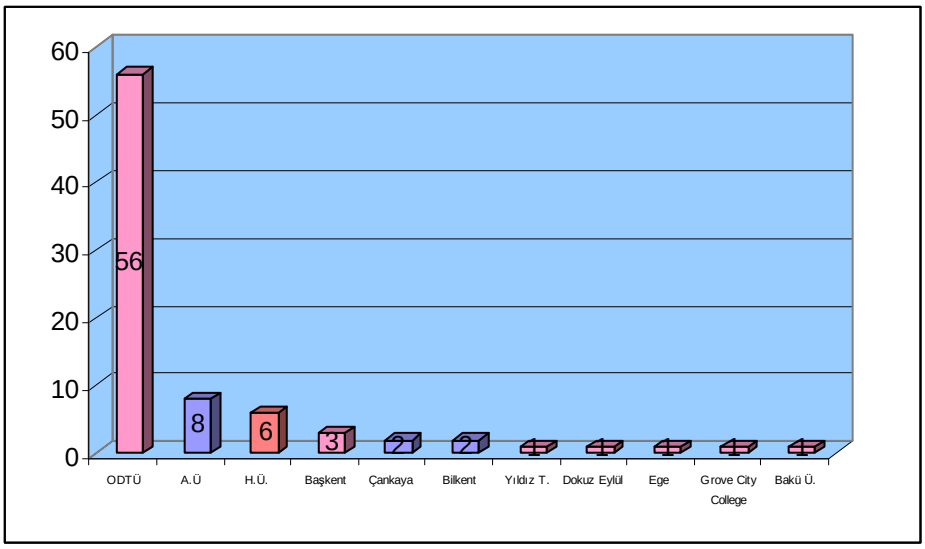


2005-2006 I. DÖNEM KABUL EDİLEN ÖĞRENCİLER





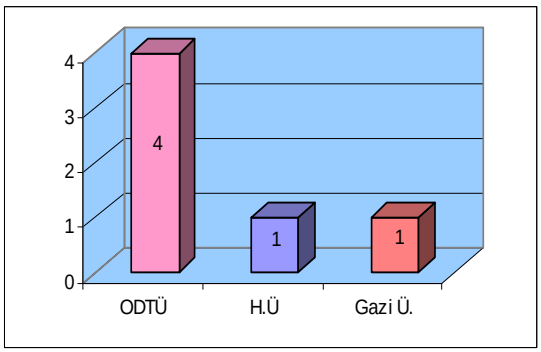
UME ÖĞRENCİLERİNİN MEZUN OLDUKLARI ÜNİVERSİTELERE GÖRE DAĞILIMI



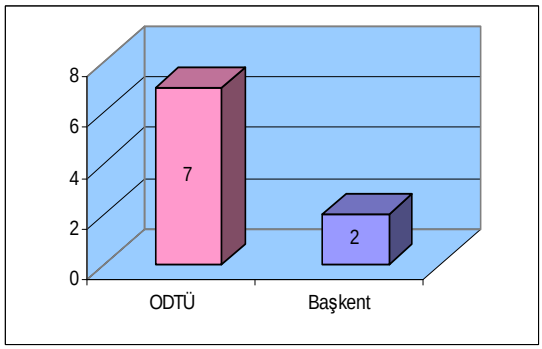
UME'YE KABUL EDİLEN ÖĞRENCİLERİN LİSANS DERECESİNİ ALDIKLARI ÜNİVERSİTELER

2004-2005 II. DÖNEM

BİLİMSEL HESAPLAMA

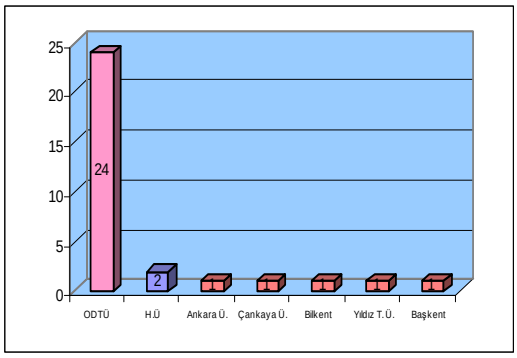


FİNANSAL MATEMATİK

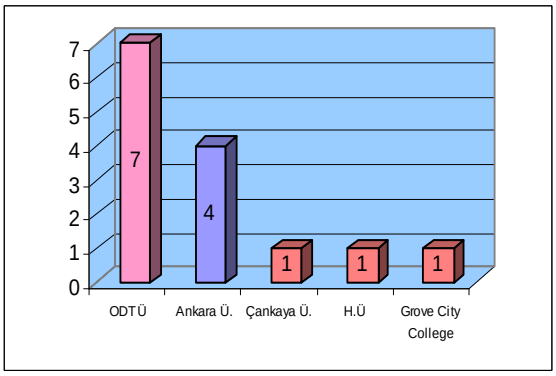


2005-2006 I. DÖNEM

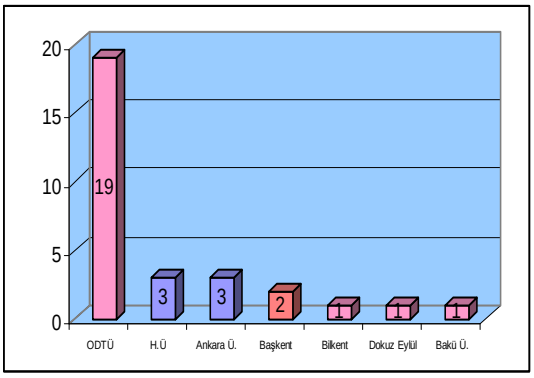
KRİPTOGRAFİ



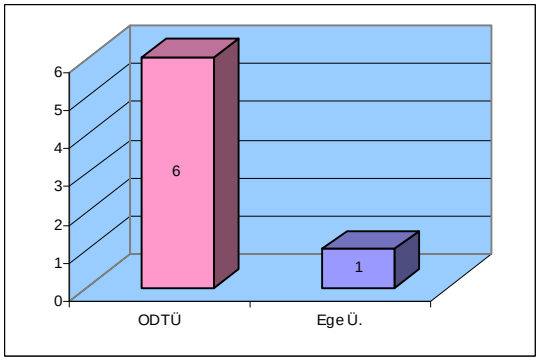
BİLİMSEL HESAPLAMA



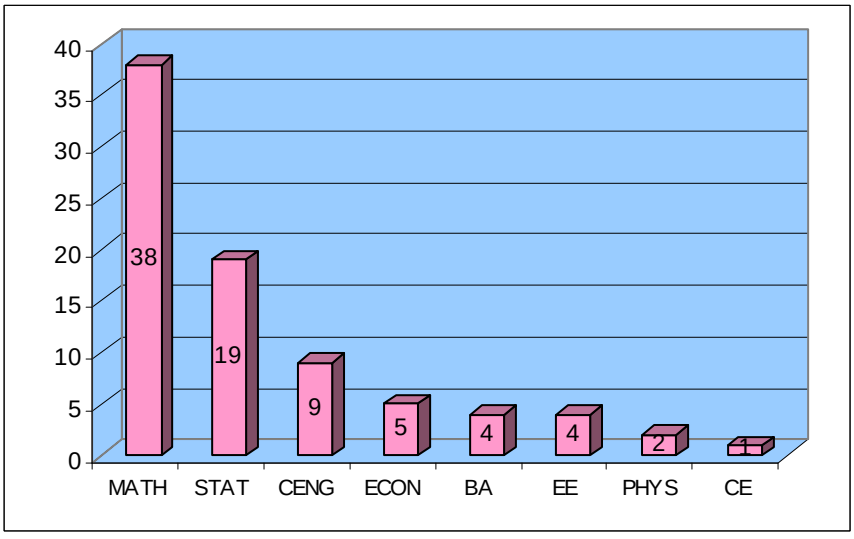
FİNANSAL MATEMATİK



HAYAT SİGORTASI



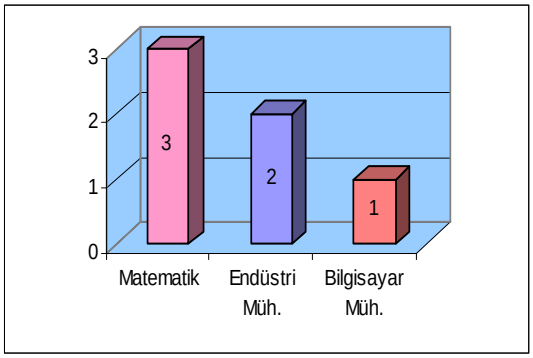
UME ÖĞRENCİLERİNİN MEZUN OLDUKLARI BÖLÜMLERE GÖRE DAĞILIMI



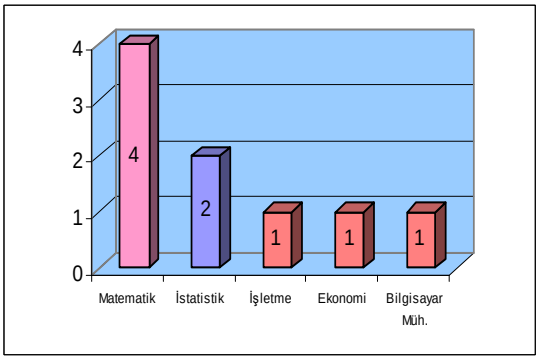
UME'YE KABUL EDİLEN ÖĞRENCİLERİN LİSANS DERECELERİNİ ALDIKLARI BÖLÜMLER

2004-2005 II. DÖNEM

BİLİMSEL HESAPLAMA

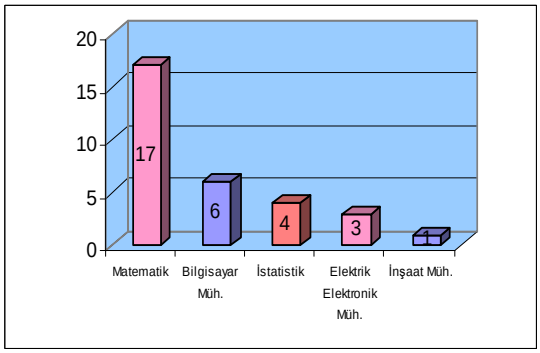


FİNANSAL MATEMATİK

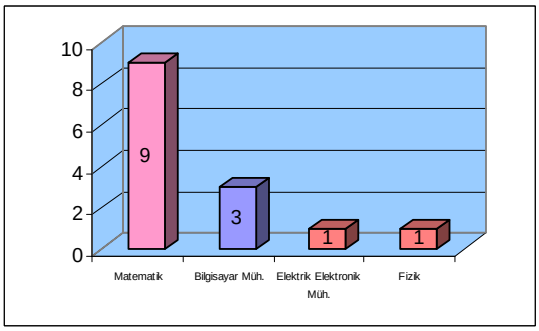


2005-2006 I. DÖNEM

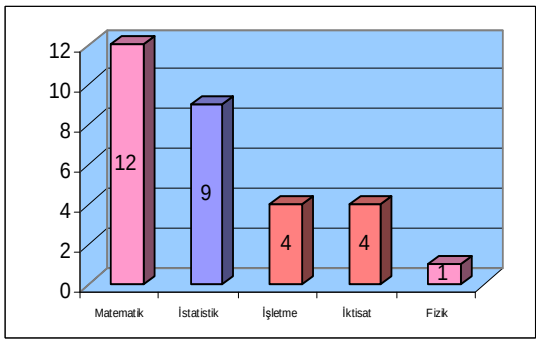
KRİPTOGRAFİ



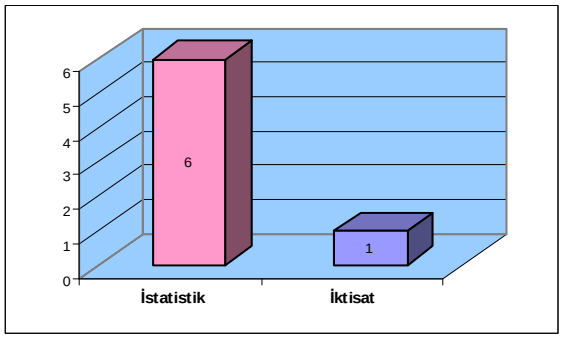
BİLİMSEL HESAPLAMA



FİNANSAL MATEMATİK

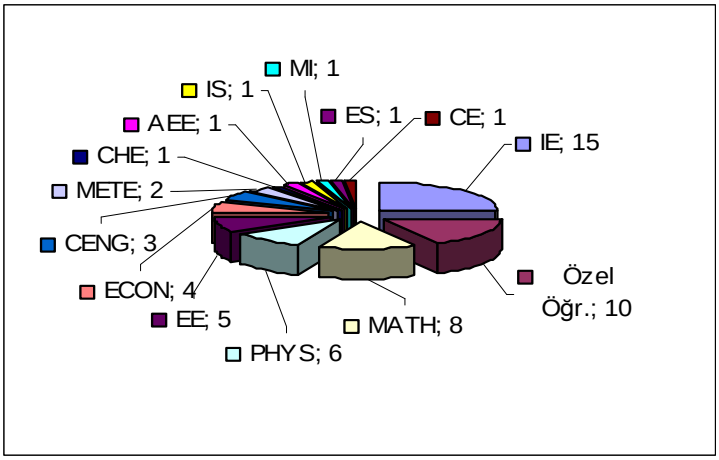


HAYATSİGORTASI



UME DERSLERİNİ ALAN UME DIŞI ÖĞRENCİLERİN BÖLÜMLERE GÖRE DAĞILIMI

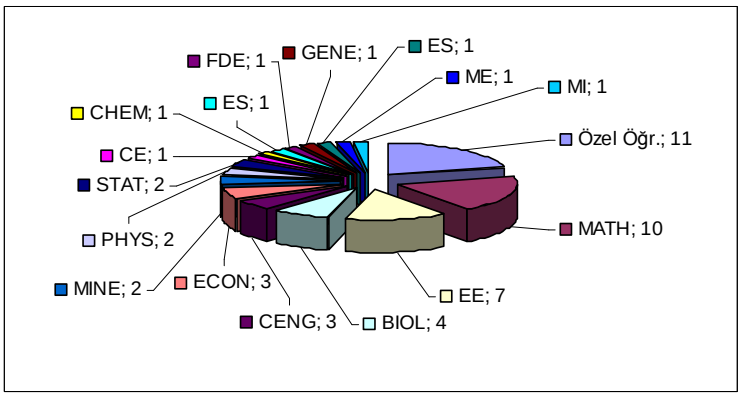
2004-2005 II.Dönem



Toplam Öğrenci Sayısı = 201

UME Dışı Öğrenci Sayısı = 59 (29%)

2005-2006 I.Dönem

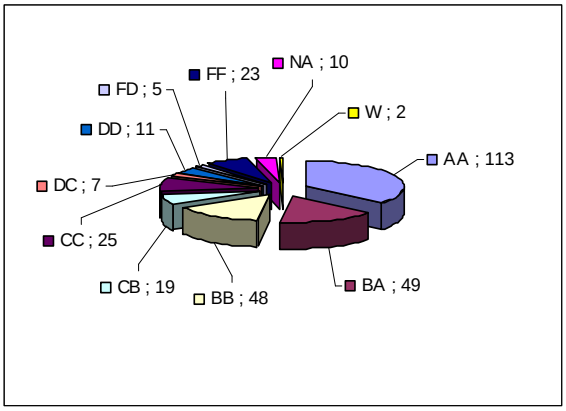


Toplam Öğrenci Sayısı = 266

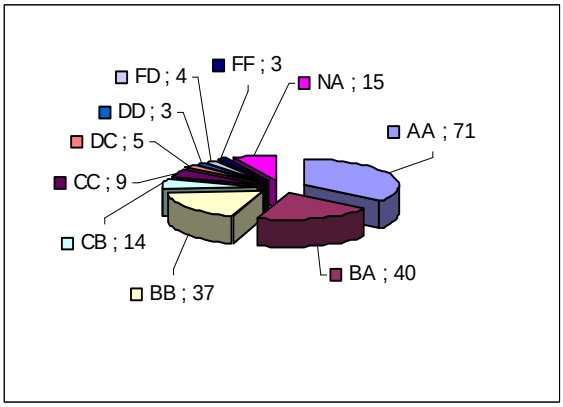
UME Dışı Öğrenci Sayısı = 52 (20%)

DÖNEMSEL VERİLEN TOPLAM NOT SAYISI

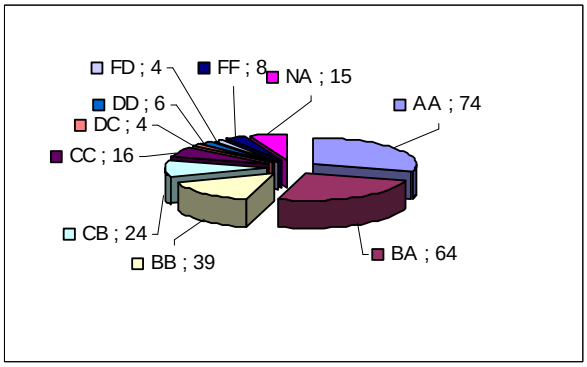
2004-2005 I.Dönem



2004-2005 II.Dönem



2005-2006 I. Dönem



EK: 5
2005 YILINDA MEZUN OLAN ÖĞRENCİLER

Kriptografi Programı

Abdulkadir Altan	"Data Sets of Block Cipher Statistical Test Kit"(Bitirme Projesi)	**Ali Doğanaksoy**
Atilla Bektaş	"Probabilistic Primality Tests" (Bitirme Projesi)	**Ali Doğanaksoy**
Baha Güçlü Dündar	"Constructions of Bent Functions and Highly Nonlinear Bolonced Boolean Functions" (Y. Lisans Tezi)	**Ali Doğanaksoy**
Barış Özkök	"An Overview of Quantum Cryptography" (Bitirme Projesi)	**Yusuf İpekoğlu**
Deniz Toz	"Evaluation Functions of Block Cipher Statistical Test Kit" (Bitirme Projesi)	**Ali Doğanaksoy**
Fatih Sulak	"Construction of Bent Functions" (Y. Lisans Tezi)	**Ali Doğanaksoy**
Mahir Ulutaş	"Notes On Systematic Authentication Codes With Highly Nonlinear Functions and Exponential Sums Over Finite Fields" (Bitirme Projesi)	**Ferruh Özbudak**
Tamer Ergun	"On factoring n with the b-algorithm" (Bitirme Projesi)	**Ali Doğanaksoy**

Bilimsel Hesaplama Programı

Arda Kurt	"Forward Problem Formulatıon In Electrocardıography Usıng a Realıstıc Torso Model" (Y. Lisans Tezi)	**Gerhard Wilhelm Weber**
Başak Akteke	"Derivative Free Optimization Methods: Application in Stirrer Configuration and Data Clustering" (Y. Lisans Tezi)	**Bülent Karasözen**
Didem Akçay	"Inference of Switching Networks by using a Piecewise Linear Formulation" (Y. Lisans Tezi)	**Gerhard Wilhelm Weber**
Mesut Taştan	"Analysis and Prediction of Gene Expression Patterns by Dynamical Systems, and by A Combinatorial Algorithm" (Y. Lisans Tezi)	**Gerhard Wilhelm Weber**
Selime Gürol	"Statistical Learning and Optimization Methods for Improving the Efficiency in Landscape image Clustering and Classification Problems"(Y. Lisans Tezi)	**Hakan Öktem**

Finansal Matematik Programı

Ayşegül İşcanoğlu	"Credit Scoring Methods And Accuracy Ratio" (Y. Lisans Tezi)	**Hayri Körezlioğlu**
Çiğdem Vural	"Moment Generating Function Approach to Pricing Interest Rate" (Bitirme Projesi)	**Hayri Körezlioğlu**
Hale Baş	"Systematic&Unsystematic Risk of Ise Industrial Companies" (Bitirme Projesi)	**Nuray Güner**
Hande Kural	"Procyclicality and Basel II" (Bitirme Projesi)	**Esma Gaygısız**
İrem Yıldırım	"Coherent and Convex Measures of Risk" (Y. Lisans Tezi)	**Hayri Körezlioğlu**
Mehmet Emre Tiftik	"Credit Risk Modeling" (Bitirme Projesi)	**Esma Gaygısız**
Nuray Çelebi	"Public Debt Management in Turkey with Stochastic Optimization Approach" (Y. Lisans Tezi)	**Coşkun Küçüközmen**
Oktay Sürücü	"Decomposition Techniques in Energy Risk Management" (Y. Lisans Tezi)	**Esma Gaygısız**
Serkan Zeytun	"Stochastic Volatility, a New Approach For Vasicek Model With Stochastic Volatility" (Y. Lisans Tezi)	**Azize Hayfavi**
Seval Çevik	"Credit Rating of Bonds, Interest Rate Processes and Modelling with a Hidden Markov Chain Model" (Bitirme Projesi)	**Gerhard Wilhelm Weber**
Zehra Ekşi	"Comparative Study of Risk Measures" (Y. Lisans Tezi)	**Hayri Körezlioğlu**
Zafer Sünger	"An Empirical Study of Greeks Approximations in Value-at-Risk Measurement for Non-linear Portfolios**"** (Bitirme Projesi)	**Coşkun Küçüközmen**
Rezzan Kan	"Value At Risk And Garch Models Assessement in Value at Risk Estimation" (Bitirme Projesi)	**Seza Danışoğlu Rhoades**

Hayat Sigortası programı

Aylin Akınlı	"A General View To The Applications Of Statistics On Motor Insurance Industry"(Bitirme Projesi)	**Irini Dimitriyadis**
Cengizhan Aksu	"Optimal Reinsurance Strategies under Exponentially Distributed Claim Amounts" (Bitirme Projesi)	**Ömer Gebizlioğlu**
Efsun Kürüm	"Annuities With Controlled Random Interest Rates" (Bitirme Projesi)	**Hayri Körezlioğlu**
G. Volkan Bilgin	Credit Derivatives Markets, Applications, Legal Issues and Strategic Use (Bitirme Projesi)	**Coşkun Küçüközmen**
Gökhan Yılmaz	"Insurer's Optimal Reinsurance Protections under Pareto Distributed Claim Amounts" (Bitirme Projesi)	**Ömer Gebizlioğlu**
Hale Taşkın İnce	"Analysis of Bauspar System and Model Based Clustering with Hidden Markov Models" (Bitirme Projesi)	**Gerhard Wilhelm Weber**
N. Ebru Buz	"Defined Benefit Pension Fund Modeling" (Bitirme Projesi)	**Sevtap Kestel& Muhammad Dabbagh**
Sema Karaaslan	"Investigating The Use of Value at Risk in Insurance (Applying Monte Carlo Simulation Method)" (Bitirme Projesi)	**Ömer Gebizlioğlu**

EK: 6
YENİ AÇILAN DERSLER

2005–2006 Güz Dönemi

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Elliptic Curves in Cryptography**
Course Code:	**IAM 505**
Credit:	**(3-0)3**
Suggested Name:	Prof. Dr. Ersan Akyıldız
Prerequisites:	Consent of the Instructor
Content:	Elliptic curves over finite fields, group structure, Weil conjectures, Super singular curves, efficient implementation of elliptic curves, determining the group order, Schoof algorithm, the elliptic curve discrete logarithm problem, the Weil pairing, MOV attack, Elliptic curve primality test, Elliptic curve factorization.
Aims:	The aim of this course is to introduce the Elliptic Curves in Cryptography. After introducing the basic facts about the elliptic curves, we shall discuss the implementation of Elliptic Curves and Algorithms to compute group order. The emphasis will be given the elliptic curve cryptosystems and the related algorithms . The other applications of Elliptic Curves in Cryptography such as primality and factorization tests will also be discussed.
Learning Outcomes:	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996.
Suggested Textbooks:	D. Hankerson, A. Menezes,S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, QA 76.9.A25, H38, 2004. 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 N. Koblitz: A Course in Number Theory and Cryptography, Springer-Verlag , 2nd edition, 1994. N. Koblitz: Algebraic Aspects of Cryptography, Vol.3, Algorithms and Computation in Mathematics, Springer-Verlag, 1998

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Basic Mathematics for Cryptography**
Course Code:	**IAM 519**
Credit:	(4-0)4
Suggested Name:	**Prof. Dr. A. Bülent EKİN, Prof. Dr. Ersan Akyıldız, Doç. Dr. Ali Doğanaksoy**
Prerequisites:	Consent of the instructor
Content:	Basic properties of Integers, Divisibility, Primes, The fundamental theorem of arithmetic, Fermat numbers, Factorization methods, Diophantine equations, Congruences, Theorems of Fermat, Euler and Wilson, Arithmetical functions, Primitive roots, Quadratic congruences, Group, Field, Field extensions, Finite fields, Factorization of polynomials, Splitting field.
Aims:	The main objective of this course is to prepare students for later studies in Cryptography Graduate Program of IAM, and also to explain some problems that are easy to ask but still unsolved and to give some ideas about why abstractions are to be made, by giving fundamental properties of integers and some algebraic preliminaries.
Outline:	WEEKS 1- 4: **The Integers:** Basic Properties, Mathematical induction, Binomial coefficients, Divisibility, Representataions of integers, Prime numbers, Greatest common divisor, Euclidean algorithm, The fundamental theorem of arithmetic, Fermat numbers and factorization methods, Linear diophantine equations, WEEKS 5- 10: **Congruences :** linear congruences, The Chinese remainder theorem, Systems of linear congruences, Applications of congruences. Theorems of Fermat, Euler and Wilson. Arithmetical functions, Primitive roots, Quadratic residues, Quadratic reciprocity. WEEK 11-14: **Algebraic Preliminaries** : Groups, Fields, Polynomials,Field extensions, Finite fields, Factorization of polynomials, Factorization of polynomials, Splitting field of a polynomial, multiple roots
Suggested Textbooks:	K. H. Rosen, Elementary Number Theory and its Applications, Addison –Wesley, 1992 David M. Burton, Elementary Number Theory, The McGraw-Hill, 1998 R. Lidl and H. Niederreiter, Finite Fields, Cambridge Univ. Pres, 1986
Resources:	A. Adler and J. E. Coury, The Theory of Numbers, Jones and Bartlett Publishers, 1995

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Selected Topics in Quantum Information Theory**
Course Code:	**IAM 702**
Credit:	**(3-0)3**
Suggested Name:	Assoc. Prof. Dr. Yusuf İpekoğlu
Prerequisites:	Consent of the instructor
Content:	Selected topics in quantum information theory. Topics will change from year to year.
Aims:	The aim of this course is to introduce students with previous exposure to basic quantum information theory to more advanced topics.
Suggested Textbooks:	There are no text books
Outline:	WEEKS 1-3: Review of basic quantum theory related to quantum information. WEEKS 3-14: Selected topics in quantum information theory, quantum computation and quantum cryptograpgy
Resources:	M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press 2000. J. Gruska, *Quantum Computing*, McGraw Hill 1999. D. Bouwmeester, A Ekert, and A. Zeilinger, *The Physics of Quantum Information*, Springer 2000. A number of review articles will also be used.

METU INSTITUTE OF APPLIED MATHEMATICS

Course Title:	**Stream Cipher Cryptanalysis**
Course Code:	**IAM 705**
Credit:	(3-0) 3
Suggested Name:	Orhun Kara
Prerequisites:	Consent of instructors
Content:	The course is devoted to analysis of stream ciphers, mostly binary additive stream ciphers. We focus on synchronous stream ciphers and LFSR based key stream generators (KSG). The classical analysis methods are covered: Linear complexity, Berlakamp-Massey algorithm, linear consistency test, correlation/fast correlation attacks, linear syndrome, algebraic attacks, edit probability-Levenshtein distance attack, etc. If time permits the attacks on some modern ciphers are introduced.
Aims :	The most significant issue in cryptographic system design may be developing tools and building blocks to make the system satisfactory resistant to known or expected attacks. This common criteria requires understanding analysis methods, especially for original designs. After taking the course, students can both enhance their skills in stream cipher design and gain an active research capacity on stream cipher cryptanalysis.
Suggested Textbooks:	R.A. Rueppel: Stream Ciphers, in Contemporary Cryptology: The science of Information Integrity, G.J. Simmons, Ed., IEEE Press, 1991. M.J.B.Robshaw: Stream Ciphers. Technical Report TR-701, 2.0, RSA Laboratories, July 1995. Patric Ekdahl: On LFSR based Stream Ciphers, Ph.D Thesis, Lund University, Department of Information Tech., Sweden, 2003
Outline:	1. week: Mathematical background: Basic arithmetic on finite fields, groups, polynomials 2. week: Overview of stream ciphers: Stream ciphers, KSGs, synchronous vs self- synchronizing stream ciphers, LFSRs, PN sequences 3. week: Common statistical security requirements of keystreams and general attacks: Divide and conquer, guess and determine, resync. attacks, distinguishing attacks, trade off attacks, inversion attacks, periodic and statistical attacks, correlation attacks, etc. 4. week: Linear complexity profile and Berlekamp Massey algorithm 5. week: Basic correlation attack on nonlinear combiners: Siegenthaler divide and conquer attack, its complexity analysis via nonlinearity and correlation immunity 6. week: Subkey guessing attacks on LFSR based ciphers: Linear consistency test Cryptanalysis of filtering generators: Linear span, linear approximation, correlation attacks 8. & 9. week: Fast correlation attacks and their improvements: Two algorithms of Meier and Staffelbach, noisy decoding problem, linear syndrome algorithm and its improvement, convolutional codes and the method of Johansson and Johnsson, fast correlation attacks based on iterative decoding algorithms 10. week: Algebraic attacks: XL/XSL algorithms, constructing MQ equations from ciphers 11. & 12. week: Correlation analysis of clock controlled generators: unconstrained embedding attacks, edit probability attacks, constrained Levenshtein distance attack 13. & 14. week: Cryptanalysis of some modern ciphers: A5, Sober-t16/t32, E_0/Bluetooth, Snow, RC4 etc.
Resources:	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: Nonlinear Feedback Shift Registers**
Course Code:	**IAM 709**
Credit:	(3-0)3
Suggested Name:	Dr. Muhiddin Uğuz, Doç. Dr. Ali Doğanaksoy
Prerequisites:	Consent of the Instructor.
Content:	Nonlinear Feedback Shift Registers: Generating Functions, and Families of Recurring Sequences, Characterizations and Properties of Nonlinear Recurring Sequences. Boolean Functions, Linear Complexity and Nonlinear Complexity(span). Combining NFSR's. Stream Ciphers Using NFSRs. GRAIN.
Aims:	The aim of this course is to introduce the students to some recent research areas in cryptography related with stream ciphers. The emphasis will be on nonlinear feedback shift register and their properties. Also design criteria for stream ciphers using NFSR's and their cryptanalysis will be discussed.
Suggested Textbooks:	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography. CRC Press, 1996.
Outline:	WEEK 1 Introduction to Nonlinear Feedback Shift Registers. WEEK 2 Boolean Functions and their Properties. WEEKS 3-5 Properties of Nonlinear Feedback Shift Registers, their Periods Linear Complexities and Nonlinear Complexities WEEKS 6-8 Characterizations of Nonlinear Feedback Shift Registers WEEKS 9-11 Designing stream ciphers using NFSRs. WEEK 12-14Cryptanalysis of stream ciphers using NFSR.

EK: 7
2005 YILINDA AÇILAN DERSLERİN LİSTESİ

2005–2006 I. Döneminde verilen dersler

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı IAM	Diğ.	Top.
Kriptografi	IAM 501	Introduction to Cryptography	Melek Yücel	9	5	14
	IAM 503	Applications of Finite Fields	Ferruh Özbudak	9	7	16
	IAM 505	Elliptic Curves in Cryptography	Ersan Akyıldız	8	-	8
	IAM 519	Basic Mathematics for Cryptography	Ali Bülent Ekin	10	2	12
	IAM 530	Elements of Statistics and Probability	Gül Ergün	20	1	21
	IAM 702	Selected Topics in Quantum Information Theory	Yusuf İpekoğlu	2	2	4
	IAM 705	Stream Cipher Cryptanalysis	Orhun Kara	12	-	12
	IAM 707	Special Topics: Block Ciphers	Ali Doğanaksoy	8	-	8
	IAM 709	Special Topics: Introduction Nonlinear Feedback Shift Registers	Muhiddin Uğuz, Emrah Çakçak	5	-	5

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı IAM	Diğ.	Top.
Bilimsel Hesaplama	IAM 529	Applied Nonlinear Dynamics	Bülent Karasözen Ömür Uğur	7	2	9
	IAM 557	Statistical Learning and Simulation	G.W.Weber	6	11	17
	IAM 561	Introduction to Scientific Computing I	Tanıl Ergenç	15	3	18
	IAM 564	Basic Algorithms and Programming	Hakan Öktem	8	4	12
	IAM 567	Mathematical Modelling	Bülent Karasözen Hakan Öktem	8	-	8
	IAM 568	Mathematical Modelling of Transport Phenomena	Yusuf Uludağ	5	-	5
	IAM 665	Advanced Continuous Optimization	G. W. Weber	2	5	7

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı IAM	Diğ.	Top.
Finansal Matematik	IAM 521	Financial Management	Seza Danışoğlu	17	1	18
	IAM 524	Financial Economics	Esma Gaygısız	14	2	16
	IAM 530	Elements of Statistics and Probability	Gül Ergün	20	1	21
	IAM 541	Probability Theory	Azize Hayfavi	13	2	15
	IAM 543	Regulation and Supervision of Risks	Coşkun Küçüközmen	9	-	9
	IAM 544	Financial Risk Assessment	Kasırga Yıldırak	7	-	7
	IAM 554	Interest Rate Models	Hayri Körezlioğlu	6	-	6
	IAM 556	Simulation	İnci Batmaz	7	4	11
	IAM 582	Life Insurance Mathematics	Muhammed Dabbagh	6	-	6
	IAM 584	Advanced Actuarial Mathematics	Ömer Gebizlioğlu	4	-	4

2004–2005 II. Döneminde verilen dersler

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Kriptografi	IAM 502	Stream Ciphers	Ali Doğanaksoy	12	2	14
	IAM 504	Public Key Cryptography	Ersan Akyıldız	10	5	15
	IAM 510	Quantum Cryptography	Yusuf İpekoğlu	1	6	7
	IAM 704	Special Topics in Cryptography: Selected Topics in Hash Functions	Ferruh Özbudak	5	-	5
	IAM 706	Special Topics: Selected Topics in Cryptoanalysis of Symmetric Cipher Systems	Orhun Kara	7	5	12

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Bilimsel Hesaplama	IAM 562	Introduction to Scientific Computing II	Tanıl Ergenç	5	2	7
	IAM 565	Introduction to Algorithms and Complexity	Ömür Uğur	1	3	4
	IAM 566	Numerical Optimization	Bülent Karasözen	7	25	32
	IAM 570	Hybrid Systems	Hakan Öktem	5	1	6
	IAM 664	Inverse Problems	G.-W. Weber	20	13	33

Anabilim Dalı	Dersin Kodu	Dersin Adı	Öğretim Üyesi	Öğr. Sayısı		
				IAM	Diğ.	Top.
Finansal Matematik	IAM 520	Financial Derivatives	Nuray Güner Adil Oran	28	1	29
	IAM 522	Stochastic Calculus for Finance	Azize Hayfavi	16	-	16
	IAM 526	Time Series Applied to Finance	Coşkun Küçüközmen	17	8	25
	IAM 554	Interest Rate Models	Hayri Körezlioğlu	5	-	5
	IAM 583	Pension Fund Mathematics	Ömer Gebizlioğlu	4	-	4
	IAM 612	Financial Modeling with Jump Processes	Nicolas Privault	4	-	4

EK: 8
STAJ YAPILAN KURUMLAR

STAJ YAPILAN KURUMLAR

Adı Soyadı	Staj Yapılan Kurum
Tolga Aktürk	İstanbul Menkul Kıymetler Borsası
Seval Çevik	Şekerbank T.A.Ş Genel Müdürlüğü
Serkan Zeytun	İstanbul Menkul Kıymetler Borsası
Gökhan Yılmaz	İstanbul Menkul Kıymetler Borsası
Utku Bora Geyikçi	İstanbul Menkul Kıymetler Borsası