

Tezli Yüksek Lisans Programı

IAM 503 Applications of Finite Fields
IAM 504 Public Key Cryptography
IAM 512 Block Ciphers
IAM 500 M.S. Thesis (non-credit)
IAM 590 Graduate Seminar (non-credit)

4 elective courses

Tezsiz Yüksek Lisans Programı

IAM 501 Introductions to Cryptography
IAM 503 Applications of Finite Fields
IAM 504 Public Key Cryptography
IAM 511 Algorithms and Complexity
IAM 512 Block Ciphers
IAM 589 Term project (non-credit)
IAM 590 Graduate Seminar (non-credit)

4 elective courses

Doktora Programı

IAM 600 Ph.D. Thesis (non-credit)
IAM 590 Graduate Seminar (non-credit)

7 elective courses

Seçmeli Dersler

IAM 501 Introductions to Cryptography
IAM 502 Stream Ciphers
IAM 511 Algorithms and Complexity
IAM 505 Elliptic Curves in Cryptography
IAM 506 Combinatorics or
MATH 405 Combinatorics
IAM 507 Algorithmic Graph Theory
IAM 508 Computer Algebra
IAM 509 Algebraic Aspects of Cryptography
IAM 510 Quantum Cryptography
IAM 602 Algebraic Geometric Codes
IAM 603 Computational Number Theory
MATH 515 Commutative Algebra

MATH 522 Coding Theory or
EE 534 Coding Theory
MATH 523 Algebraic Number Theory
MATH 524 Theory of Function Fields
EE 435 Telecommunications I
EE 436 Telecommunications II
EE 533 Information Theory
EE 542 Computer Networks
CENG 530 Computer Networks and
Communications
CENG 559 Data Security and Protection
CENG 565 Introduction to Theory of
Computation
CENG 567 Design and Analysis of
Algorithms
CENG 573 Symbolic Algebraic Computation
CENG 575 Simulation Modeling and
Analysis
CENG 577 Parallel Computing

Adres

Orta Doğu Teknik Üniversitesi
Uygulamalı Matematik Enstitüsü
Dumlupınar Blv. No:1, 06800 Çankaya
Ankara/TÜRKİYE

Telefon

+90 312 210 29 87

Fax

+90 312 210 29 85

E-mail

www.iam@metu.edu.tr

Website

<http://iam.metu.edu.tr/>



Kriptografi

Yüksek Lisans ve Doktora Programı



ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Neden Kriptografi?

Kriptografi bilgi güvenliğinde ve özellikle siber güvenlikte önemli bir role sahiptir. Bilginin güvenli, bütün ve aslına uygun halde aktarımı ve saklanması matematiksel tekniklerin kullanılmasıyla gerçekleşir. Bilgi sistemleri arasında bağlantı arttıkça ve bu sistemlere erişim küresel boyuta ulaştığı sürece şüpheli birçok saldırıya karşı bilginin korunması gereksinimi önem arz edecektir.

Türkiye’de Kriptografi’nin Önemi

Siber güvenliğin ana araçlarından olan kriptografi teknikleri ulusal güvenliğin sağlanması açısından önemlidir. Kriptografik algoritmaların ve protokollerin güvenliğinin onaylanması için kriptografi uzmanlığı gereklidir. Farklı sektörlerde çalışma gösteren birçok kuruluş bilginin olası saldırılara karşı korunması için çaba sarf etmektedir ki bu durum yetenekli kriptografi uzmanlarına duyulan ihtiyacın artan seviyede olduğunu kanıtlamaktadır.

Kriptografi Programının Amaçları

- Kriptografi alanında uluslararası tanınan özgün programlar yürütmek; yüksek lisans ve doktora dereceleri vermek.
- Simetrik ve asimetrik kriptografinin pratik uygulamalarına matematiksel yöntemlerle yenilikler katmak.
- Uygulamacılara en yeni teknik ve algoritmalar için ihtiyaç duydukları matematiksel araçları tanıtmak.
- Kriptografi ve bilgi güvenliği alanlarında uluslararası boyutta tanınmış bir araştırma merkezi olmak.

Kimler Programa Katılabilir?

Kriptografi, matematik, bilgisayar bilimleri/mühendisliği, elektrik ve elektronik mühendisliği, istatistik ve fizik alanlarına dayanan çok disiplinli bir program olup tasarım, güvenlik analizi ve kriptografik algoritmaların uygulanması çalışmalarına odaklanmaktadır.

İş Olanakları

- Türk Silahlı Kuvvetleri
- TÜBİTAK-BİLGEM
- ULAKBİM
- ÖSYM
- ASELSAN
- HAVELSAN
- Başbakanlık
- Üniversiteler
- Siber güvenlik ve bilgi güvenliği alanlarındaki yazılım şirketleri

Kabul Şartları ve Başvuru

Başvuru için aşağıdaki belgeler gereklidir:

- ODTÜ-İYS (İngilizce Yeterlilik Sınavı) ≥ 65 ya da TOEFL-IBT ≥ 79
- ALES ≥ 75 ya da GRE-Sayısal Puan ≥ 713
- En az 2 referans mektubu
- Niyet mektubu

Programa son başvuru tarihi: 22 Haziran 2017

IYS Son başvuru tarihi: 07 Haziran 2017

Gerekli görüldüğü takdirde mülakat yapılabilir.

Daha fazla bilgi için:

<http://iam.metu.edu.tr/universitys-application-page>

ENSTİTÜ ÖĞRETİM GÖREVLİSİ

CENK, Murat: B.S. METU; M.S. Çankaya University; Ph.D. METU.

BAĞLANTILI ENSTİTÜ ÖĞRETİM GÖREVLİSİ

AKLEYLEK, Sedat: B.S. Ege University; M.S., Ph.D. METU.

AKYILDIZ, Ersan: B.S. METU; Ph.D. University of British Columbia.

BİLHAN, Mehpare: B.S. METU; Ph.D. University Paris VI (Pierre-e-Marie Curie).

DOĞANAKSOY, Ali: B.S. İstanbul Technical University; M.S., Ph.D. METU.

GÜLER, İ. Yurdahan: B.S., M.S., Ph.D. METU.

ÖZBUDAK, Ferruh: B.S., M.S., Ph.D. Bilkent University.

SAYGI, Zülfükar: B.S., M.S., Ph.D. METU.

UĞUZ, Muhiddin: B.S. METU; M.S. Michigan State University; Ph.D. METU.

YALÇIN, Tolga: B.S., M.S. METU; Ph.D. EPFL.

YAYLA, Oğuz: B.S., M.S., Ph.D. METU.

YILMAZ, Abdürrahim: B.S. METU; MS., Ph.D. Hacettepe University.

YÜCEL, Melek: B.S., M.S., Ph.D. METU.