Tezli Yüksek Lisans Programı

IAM 503 Applications of Finite Fields
IAM 504 Public Key Cryptography
IAM 512 Block Ciphers
IAM 500 M.S. Thesis (Kredisiz)
IAM 698 Ethics and Research Methods (Kredisiz)
IAM 590 Graduate Seminar (Kredisiz)

4 seçmeli ders

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 (Kredisiz)
IAM 698 Ethics and Research Methods (Kredisiz)
IAM 590 Graduate Seminar (Kredisiz)

5 seçmeli ders

Doktora Programı

IAM 600 Ph.D. Thesis (Kredisiz)
IAM 698 Ethics and Research Methods (Kredisiz)
IAM 690 Graduate Seminar (Kredisiz)

7 seçmeli ders

Lisans Sonrası Doktora Programı

IAM 503 Applications of Finite Fields
IAM 504 Public Key Cryptography
IAM 512 Block Ciphers
IAM 600 Ph.D. Thesis (Kredisiz)
IAM 698 Ethics and Research Methods (Kredisiz)
IAM 690 Graduate Seminar (Kredisiz)

11 seçmeli ders

Seçmeli Dersler

IAM 501 Introduction to Cryptography
IAM 502 Stream Ciphers
IAM 505 Elliptic Curves in Cryptography
IAM 506 Combinatorics
IAM 507 Algorithmic Graph Theory
IAM 508 Computer Algebra
IAM 509 Algebraic Aspects of Cryptography
IAM 510 Quantum Cryptography
IAM 511 Algorithms and Complexity
IAM 602 Algebraic Geometric Codes
IAM 603 Computational Number Theory
IAM 701 Security Tests in Cryptography
IAM 711 Elliptic Curve Cryptography
IAM 715 Cryptography and Coding Theory
IAM 718 Block Cipher Cryptanalysis
IAM 729 Normal Bases in Finite Fields
IAM 730 Quantum Information Theory
IAM 732 Applied Cryptography for Cyber Security
IAM 736 Introduction to Cryptographic Engineering
IAM 737 Quantum Cryptography

UYGULAMALI MATEMATİK ENSTİTÜSÜ
Adres : Dumlupınar Blv. No:1, 06800
Çankaya/Ankara, Turkey
Telefon : +90 (312) 210 2987
Fax : +90 (312) 210 2985
E-Mail : iamenst@metu.edu.tr
Website: https://iam.metu.edu.tr/cryptography

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 kriptografik teknikler, 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 verilmesi amaçlanmaktadır.
Simetrik ve asimetrik kriptografinin pratik uygulamalarına matematiksel yöntemlerle yenilikler katılması hedeflenmektedir.
Uygulamacılara en yeni teknik ve algoritmalar için ihtiyaç duydukları matematiksel araçları tanıtmak önem taşır.
Kriptografi ve bilgi güvenliği alanlarında uluslararası boyutta tanınmış bir araştırma merkezi olmak programın önemli bir amacıdır.

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

Eğitim süresince öğrencilere projelerde görev alma imkanı sağlanmaktadır.

Kriptografi mezunları, TÜBİTAK-BİLGEM, TÜBİTAK-ULAKBİM, ASELSAN, HAVELSAN, ÖSYM, kamu kurumları, siber güvenlik ve bilgi güvenliği alanındaki yazılım şirketlerinde ile yurt içi ve yurt dışında akademisyen olarak çalışabilmektedir.

Kabul Şartları ve Başvuru

Başvuru için aşağıdaki belgeler gereklidir:

- **İngilizce Yeterlilik:** ODTÜ-İYS ≥ 64.5 veya TOEFL ≥ 79
- **Sınav:**
  M.Sc.: ALES ≥ 70 veya
  GRE-quant. ≥ 155 (GRE-quant. ≥ 696)
  Ph.D.: ALES ≥ 75 veya
  GRE-quant. ≥ 156 (GRE-quant. ≥ 713)
- **Referans Mektubu** En az 2 tane.
- **Niyet Mektubu**
- Gerek görüldüğü takdirde **mülakat** yapılabilir.

Programa ve IYS son başvuru tarihi genellikle Haziran ayı içindedir. Bu nedenle aşağıdaki web sayfasından son başvuru tarihlerini izlemeniz önerilir.
http://iam.metu.edu.tr/application-and-admission

ENSTİTÜ ÖĞRETİM ÜYESİ

CENK, Murat

BAĞLANTILI ENSTİTÜ ÖĞRETİM ÜYESİ

AKLEYLEK, Sedat: Bilgisayar Müh., Ondokuz Mayıs Üniversitesi

AKYILDIZ, Ersan: Matematik, ODTÜ

BİLGİN, Begül: KU LEUVEN

BİLHAN, Mehpare: Matematik, ODTÜ

DOĞANAKSOY, Ali: Matematik, ODTÜ

GÜLER, İ. Yurdahan: UME, ODTÜ

KAVUT, Selçuk: Bilgisayar Müh., Balıkesir Üniversitesi

KIRLAR, Barış B.: Matematik, Süleyman Demirel Üniversitesi

MANGUOĞLU, Murat: Bilgisayar Müh. ODTÜ

MESNAGER, Sihem: University of Paris

ERTAN, Onur: Bilgisayar Müh. ODTÜ

ÖZBUDAK, Ferruh: Matematik, ODTÜ

SAYGI, Zülfikar: Matematik, TOBB Üniversitesi

SELÇUK, Ali Aydın: Bilgisayar Müh., TOBB Üniversitesi

SINAK, Ahmet: Matematik-Bilgisayar Bilimleri, Necmettin Erbakan Üniversitesi

SULAK, Fatih: Matematik, Atılım Üniversitesi

TEKİN, Eda: Matematik, Karabük Üniversitesi

TEZCAN, Cihangir: Matematik, ODTÜ

UĞUZ, Muhiddin: Matematik, ODTÜ

YAYLA, Oğuz: Matematik, Hacettepe Üniversitesi

YILMAZ, Abdürrahim: Matematik, ODTÜ