M.S. Thesis Program

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

4 elective courses

M.S. Non-Thesis Program

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 698 Ethics and Research Methods (non-credit)
IAM 590 Graduate Seminar (non-credit)

5 elective courses

Ph.D. Program

IAM 600 Ph.D. Thesis (non-credit)
IAM 568 Ethics and Research (non-credit)
IAM 690 Graduate Seminar (non-credit)

7 elective courses

Integrated Ph.D. Program

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

11 elective courses

Elective Courses

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

INSTITUTE OF APPLIED MATHEMATICS
Address: Dumlupınar Blv. No:1, 06800
Çankaya/Ankara, Turkey
Phone : +90 (312) 210 2987
Fax : +90 (312) 210 2985
E-Mail : iamenst@metu.edu.tr
Website: https://iam.metu.edu.tr/cryptography

Cryptography

M.Sc. & Ph.D. Programs

ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

Why Study Cryptography?

Cryptography is an important component of information security and plays an important role especially in cyber security. It encompasses mathematical techniques for providing confidentiality, integrity and authenticity of data during transmission and storage. As the information systems get connected and become accessible globally, protecting data susceptible to attacks of various kinds becomes more important.

Importance of Cryptography in Turkey

Cryptographic techniques which are one of the main tools in cyber security are crucial for the national security. Cryptographic expertise is required for verifying the security of cryptographic algorithms and protocols. All kinds of institutions dealing with sensitive data should be guarded against attacks. Hence there is a demand for highly skilled cryptographers.

Objectives of Cryptography Program

The objectives of the Cryptography Graduate Program are to conduct a graduate program leading to M.Sc. and Ph.D. degrees in the field of Cryptography, to provide a mathematical treatment to the practical aspects of cryptography, to introduce mathematical tools needed for the latest techniques and algorithms to the serious practitioners, to foster and support interdisciplinary research in the field, and to be an internationally recognized center for research in cryptography and related areas of information security.

Suitable for Students from all Disciplines

Cryptography is a multidisciplinary program based on mathematics, computer science/engineering, electrical and electronics engineering, statistics and physics, which focuses on design, security analysis, and implementations of cryptographic algorithms.

Job Opportunities

Students in the Cryptography Program, may find positions in research projects.

The graduates mainly work and take part in Turkish Armed Forces, TUBITAK-BİLGEM, TUBITAK-ULAKBIM, ASELSAN, HAVELSAN, ÖSYM, universities, and software companies in the area of cyber security and information security.

Admission Requirements and Application

The selection process requires documentation of the followings:

- **English Proficiency:** METU-EPE ≥ 64.5 or TOEFL ≥ 79
- **Graduate Exam:**
  M.Sc.: ALES ≥ 70 or
  GRE-quant. ≥ 155 (GRE-quant. ≥ 696)
  Ph.D.: ALES ≥ 75 or
  GRE-quant. ≥ 156 (GRE-quant. ≥ 713)
- **Reference Letters:** At least 2.
- **Letter of intention**
- **Oral Interview** if necessary.

Usually, the application deadline to program and EPE is June.
For application deadline and more information:
http://iam.metu.edu.tr/application-and-admission

FACULTY

CENK, Murat

AFFILIATED FACULTY

AKLEYLEK, Sedat: Computer Eng., Ondokuz Mayıs University

AKYILDIZ, Ersan: Mathematics, METU

BİLGİN, Begül: KU LEUVEN

BİLHAN, Mehpare: Mathematics, METU

DOĞANAKSOY, Ali: Mathematics, METU

GÜLER, İ. Yurdahan: IAM, METU

KAVUT, Selçuk: Computer Eng., Balıkesir University

KIRLAR, Barış B.: Mathematics, Süleyman Demirel University

MANGUOĞLU, Murat: Computer Eng., METU

MESNAGER, Sihem: University of Paris

ONUR Ertan: Computer Eng., METU

ÖZBUDAK, Ferruh: Mathematics, METU

SAYGI, Zülfikar: Mathematics, TOBB University

SELÇUK, Ali Aydın: Computer Eng., TOBB University

SINAK, Ahmet: Mathematics-Computer Science, Necmettin Erbakan University

SULAK, Fatih: Mathematics, Atılım University

TEKİN, Eda: Mathematics, Karabük University

TEZCAN, Cihangir: Mathematics, METU

UĞUZ, Muhiddin: Mathematics, METU

YAYLA, Oğuz: Mathematics, Hacettepe University

YILMAZ, Abdürrahim: Mathematics, METU