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 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 590 Graduate Seminar (non-credit)

4 elective courses

Ph. D. Program

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

7 elective courses

Elective Courses

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

Address
Middle East Technical University
Institute of Applied Mathematics
Dumlupınar Blv. No:1, 06800 Çankaya
Ankara/TURKEY

Telephone
+90 312 210 29 87

Fax
+90 312 210 29 85

E-mail
wwwiam@metu.edu.tr

Website
http://iam.metu.edu.tr/

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 conventional and public-key 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.
- 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

The graduates mainly work and take part in Turkish Armed Forces, TUBITAK-BİLGEM, ULAKBİM, ÖSYM, Aselsan, Havelsan, National Intelligence Service, 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:

- METU-EPE (English Proficiency Exam) ≥ 65 or TOEFL-IBT ≥ 79
- ALES ≥ 75 or GRE-Quantitative Score ≥ 713
- At least 2 reference letters
- Letter of intention

Application Deadline to program: June 22, 2017
Application Deadline to EPE: June 07, 2017
Applicants will be interviewed when necessary.
For application deadline and more information:

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

FACULTY

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

AFFILIATED FACULTY

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.