CRYPTOGRAPHY PROGRAM

Why Applied Mathematics?

Mathematics is creative, exciting and is the future. Without mathematics, modern key technologies would be unimaginable.

Institute of Applied Mathematics (IAM) was established in 2002 at METU to educate graduates from various disciplines with the objective of developing and applying their skills for solving real life problems in science, engineering, finance and industry.

About 50 scientists from different fields contribute to teach and research at the IAM and 277 students graduated since 2004, among them 45 with Ph.D. degrees.

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 is 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.

Why Cryptography at METU?

METU was ranked in the top 80 among the world's most reputable 100 universities in the last three years according to "The Times Higher Education World Reputation Rankings".

METU was also ranked among the Top Universities in the World in 9 subjects according to Quacquarelli Symonds (QS) of UK. Mathematics, Statistics-Operations Research, Economics-Econometrics, Computer Science and Information Systems are the subjects in the top 200 university list in 2014, which are the interdisciplinary research areas of the IAM.

METU has knowledgeable and valuable academic staffs who are experts in interdisciplinary teaching and research areas. The language of education is English.

A total number of 105 students are graduated with Ph.D. and M.Sc. degrees in Cryptography Program since 2004.

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 Diciplines

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.

ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

UYGULAMALI MATEMATİK ENSTİTÜSÜ
INSTITUTE OF APPLIED MATHEMATICS

CRYPTOGRAPHY PROGRAM

Structure of the Graduate Program

The program offers M.Sc. degree with thesis, non-thesis options and Ph.D. degree. Students having insufficient mathematical background are required to take deficiency courses.

Core Courses*

IAM 501 Introduction to Cryptography
IAM 502 Stream Ciphers
IAM 503 Applications of Finite Fields
IAM 504 Public Key Cryptography
IAM 511 Algorithms and Complexity
IAM 512 Block Ciphers

Selected Elective Courses*

IAM 505 Elliptic Curves in Cryptography
IAM 506 Combinatorics
IAM 509 Algebraic Aspects of Cryptography
IAM 510 Quantum Cryptography
IAM 705 Stream Cipher Cryptanalysis
IAM 715 Cryptography and Coding Theory
IAM 717 Cryptological Characteristics of Boolean Functions and S-Boxes
IAM 718 Block Cipher Cryptanalysis
IAM 719 Algorithmic Number Theory
IAM 732 Applied Cryptography for Cyber Security
IAM 733 Cryptographic Protocols
IAM 736 Introduction to Cryptographic Engineering

*Students are encouraged to take courses from computer engineering and electrical and electronics engineering.
http://iam.metu.edu.tr/courses

Collaboration and Student Exchange

- Academic collaborations with 13 universities
- TUBİTAK - UEKAE
- Erasmus Mundus Exchange Agreements

Projects

- DPT - Cryptographic Algorithm Design, Analysis and Implementation
- ASELSAN Projects:
  - Selecting Secure Elliptic Curves over GF(p) and Implementing a Signature System Based on Elliptic Curves
  - Developing Statistical and Structural Test Suite Software to Evaluate the Security of Block Ciphers
- TURKTRUST A.Ş. - Security Tests for RSA Cryptosystem Parameters

Conferences Organized

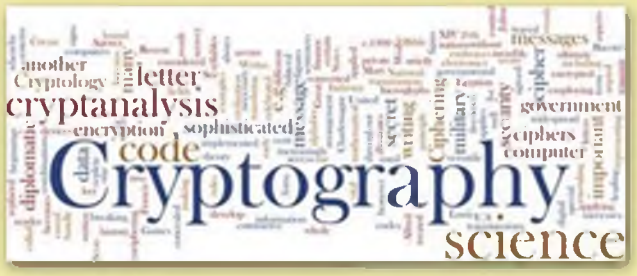
- Information Security and Cryptology Conference (ISC), 2004-2013
- Codes over Rings, Summer School, 2008
- Workshop on the Arithmetic of Finite Fields, 2010
- ICACM - International Conference on Applied and Computational Mathematics, 2012

Student Support

- Assistantship and part-time student assistantship opportunity (requires Turkish citizenship)
- Turkish Scientific Research Council (TÜBİTAK) Scholarship
- Assistantship in TÜBİTAK Research Projects
- Techno-Thesis: Joint Thesis Project with METU Techno Park
- 50% Higher Education Council (YÖK) Scholarship with the deduction Tuition fee for foreign students being successful in the program.

Job Opportunities

The graduates mainly work and take part in Turkish Armed Forces, TUBIT AK-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: June 20, 2014
Application Deadline to EPE: June 10, 2014
Applicants will be interviewed when necessary.
For application deadline and more information:
http://iam.metu.edu.tr/universitys-application-page