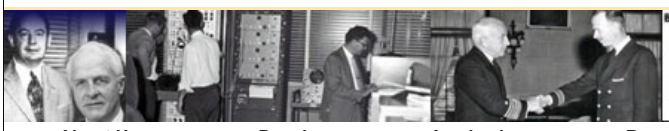
2013

Academic Certificate in the mathematics of secure communication - Curriculum 280 (archived)

Monterey, California, Naval Postgraduate School



DEPARTMENT OF APPLIED MATHEMATICS

Certificate Programs

The Department of Applied Mathematics offers academic certificate programs in Secure Communication, Scientific Computation, and Complex Networks (under development). These are four course programs that may be taken independently of a degree.

Academic Certificate in the Mathematics of Secure Communication - Curriculum 280

Click above to view the certificate brochure

Program Manager
Pantelimon Stanica
Spanagel Hall, Room 268
(831) 656-2714, DSN 756-2714
FAX (831) 656-2355
pstanica@nps.edu

Brief Overview

The Mathematics of Secure Communication certificate program comprises four courses (see below). Upon successful completion of the coursework, students will be awarded a certificate of accomplishment in keeping with standard practices of the Naval Postgraduate School. The purpose for its development is to provide Mathematics education to Naval officers and DoD civilians in the broad area of cryptography and secure communications. As such it satisfies a Knowledge, Skills, Abilities (KSA) requirement in the Applied Technology field of Fundamentals of cryptology and cryptanalysis for Professional Military Education.

Requirements for Entry

Prospective students must meet the necessary prerequisites for the courses in the program.

Entry Date

Program entry dates are flexible and students who wish to pursue this certificate should coordinate with the program manager.

Program Length

Variable.

MA Academic Certificate Requirements

To earn the academic certificate students must pass all four courses with a C+ (2.3 Quality Point Rating (QPR)) or better in each course and an overall QPR of 3.0 or better. Students earning grades below these standards will need to retake the courses to bring their grades within standards or they will be withdrawn from the program.

Required Courses

MA3025 - Logic and Discrete Mathematics (4-1)
MA3025 provides a rigorous foundation in logic and elementary discrete mathematics to students of mathematics and computer science. Topics from logic include modeling English propositions, propositional calculus, quantification, and elementary predicate calculus. Additional mathematical topics include elements of set theory, mathematical induction, relations and functions, and elements of number theory.
Prerequisite: MA1025 or MA2025

MA3560 - Applied Modern Algebra and Number Theory (4-0)
This course is devoted to aspects of modern algebra and number theory that directly support applications, principally in communication. The algebraic emphasis is on ring and field theory, with special emphasis on the theory of finite fields, as well as those aspects of group theory that are important in the development of coding theory. Elements of number theory include congruences and factorization. Applications are drawn from topics of interest to DoN/DoD. These include error correcting codes and cryptography.
Prerequisite: MA3025

MA4560 - Coding and Information Theory (4-0)
Mathematical analysis of the codes used over communication channels is made. Techniques developed for efficient, reliable and secure communication are stressed. Effects of noise on information transmission are analyzed and techniques to combat their effects are developed. Linear codes, finite fields, single and multiple error-correcting codes are discussed. Codes have numerous applications for communication in the military, and these will be addressed.
Prerequisite: MA3560

MA4570 - Cryptography (4-0)
The methods of secret communication are addressed. Some simple cryptosystems are described and classical techniques of substitution and transposition are considered. The public-key cryptosystems, RSA, Discrete Logarithm and other schemes are introduced. Applications of cryptography and cryptanalysis.
Prerequisite: MA3560

Additionally, the students in the program can register in

MA4026 Combinatorial Mathematics (4-0)

Advanced techniques in enumerative combinatorics and an introduction to combinatorial structures. Topics include generating functions, recurrence relations, elements of Ramsey theory, theorems of Burnside and Polya, and balanced incomplete block designs. Application areas with DoD/DoN relevance range from mathematics to computer science and operations research, including applications in probability, game theory, network design, coding theory, and experimental design. Prerequisites: MA3025.

MA4027 Graph Theory and Applications (4-0)
Advanced topics in the theory of graphs and digraphs. Topics include graph coloring, Eulerian and Hamiltonian graphs, perfect graphs, matching and covering, tournaments, and networks. Application areas with DoD/DoN relevance range from mathematics to computer science and operations research, including applications to coding theory, searching and sorting, resource allocation, and network design. Prerequisites: MA3025.

MA4550 Combinatorial and Cryptographic Properties of Boolean Functions (4-0)
The course will discuss the Fourier analysis of Boolean functions and the relevant combinatorics with an eye toward cryptography and coding theory. Particular topics will include avalanche features of Boolean functions, correlation immunity and resiliency, bentness, trade-offs among cryptographic criteria and real-life applications in the designs of stream and block ciphers.
Prerequisite: MA3025

The certificate program is self-contained, requiring only an elementary course in discrete mathematics for entry (MA1025 or MA2025 - Discrete Mathematics). This introductory course is also available to students at NPS and is planned to be offered as a web-based course.

Academic Certificate in Scientific Computation - Curriculum 283

Click above to view the certificate brochure

Program Manager
Beny Neta
Code MA/Nd, Spanagel Hall, Room 270
(831) 656-2235, DSN 756-2235
FAX (831) 656-2355
bneta@nps.edu

Brief Overview
The Scientific Computation academic certificate provides education in the use of mathematical analysis and numerical solution techniques to model science and engineering problems on computers. Scientific Computation has become the third pillar of scientific research, a peer with traditional methods of physical experimentation and theoretical investigation, and as such has emerged as an area critical to the success of the mission of the Navy and the Department of Defense. High performance computers are already widely used in weather prediction, modeling ocean dynamics, design and testing of advanced weapons systems, development of new smart materials, etc. And it has become very clear that even more broad application of scientific computation will be essential to accelerate scientific discovery for national competitiveness and global security.

A thorough understanding of the mathematics underlying the algorithms is essential for the correct interpretation and further development of computational approaches in science. The Scientific Computation certificate program is designed to provide that very background. It is comprised of four courses – the first two of these are fundamental and the other two are selected from a group of nine courses that allows the certificate to be tailored to a specific area of interest. Upon successful completion of the coursework, students will be awarded a certificate of accomplishment in keeping with standard practices of the Naval Postgraduate School.

Requirements for Entry
Prospective students must meet the necessary prerequisites for the courses in the program.

Entry Date
Program entry dates are flexible and students who wish to pursue this certificate should coordinate with the program manager.

Program Length
Variable.

MA Academic Certificate Requirements
To earn the academic certificate students must pass all four courses with a C+ (2.3 Quality Point Rating (QPR)) or better in each course and an overall QPR of 3.0 or better. Students earning grades below these standards will need to retake the courses to bring their grades within standards or they will be withdrawn from the program.

Required Courses

- **MA3046 Matrix Analysis** (4-1)
  This course provides students in the engineering and physical sciences curricula with an applications-oriented coverage of major topics of matrix and linear algebra. Matrix factorizations (LU, QR, Cholesky), the Singular Value Decomposition, eigenvalues and eigenvectors, the Schur form, subspace computations, structured matrices. Understanding of practical computational issues such as stability, conditioning, complexity, and the development of practical algorithms. Prerequisites: MA2043 and EC1010.
- **MA3232 Numerical Analysis** (4-0)
  Provides the basic numerical tools for understanding more advanced numerical methods. Topics for the course include: Sources and Analysis of Computational Error, Solution of Nonlinear Equations, Interpolation and Other Techniques for Approximating Functions, Numerical Integration and Differentiation, Numerical Solution of Initial and Boundary Value Problems in Ordinary Differential Equations, and Influences of Hardware and Software. Prerequisites: MA1115, MA2121 and ability to program in MATLAB and MAPLE.

And any two from

- **MA4237 Advanced Topics in Numerical Analysis** (V-0)
  The subject matter will vary according to the abilities and interest of those enrolled. Applications of the subject matter to DoD/DoN are discussed. Prerequisites: Consent of instructor.
- **MA4242 Numerical Solution of Ordinary Differential Equations** (4-0)
  Adams formulas, Runge-Kutta formulas, extrapolation methods, implicit formulas for stiff equations; convergence and stability, error estimation and control, order and stepsize selection, applications. Prerequisites: MA3232.
- **MA4243 Numerical Solution of Partial Differential Equations** (3-1)

Finite difference methods for parabolic, elliptic, and hyperbolic equations, multi-grid methods; convergence and stability, error estimation and control, numerical solution of finite difference equations, applications. Prerequisites: MA3132, MA3232 suggested.

- **MA4245 Mathematics Foundation of Galerkin Methods** (4-0)
  Variational formulation of boundary value problems, finite element and boundary element approximations, types of elements, stability, eigenvalue problems. Prerequisites: MA3132, MA3232 or equivalent.
- **MA4248 Computational Linear Algebra** (4-1)
  Development of algorithms for matrix computations. Rounding errors and introduction to stability analysis. Stable algorithms for solving systems of linear equations, linear least squares problems and eigen problems. Iterative methods for linear systems. Structured problems from applications in various disciplines. Prerequisites: MA3046, or consent of instructor, advanced MATLAB programming.
- **MA4261 Distributed Scientific Computing** (3-2)
  General principles of parallel computing, parallel techniques and algorithms, solution of systems of linear equations, eigenvalues and singular value decomposition, domain decomposition and application (e.g., satellite orbit determination and shallow water fluid flow). Prerequisites: MA3042 or MA3046, MA3132, and MA3232.
- **MA4311 Calculus of Variations** (3-0)
  Euler equation, Weierstrass condition, Legendre condition, numerical procedures for determining solutions, gradient method, Newton method, Transversability condition, Rayleigh Ritz method, conjugate points. Concepts are related to geometric principles whenever possible. Prerequisites: MA2121 (programming experience desirable).
- **MA4377 Asymptotic and Perturbation Methods I** (3-0)
  Advanced course in the application of approximate methods to the study of integrals and differential equations arising in physical problems. Topics covered include: asymptotic sequences and expansions, integrals of a real variable, contour integrals, limit process expansions applied to ordinary differential equations, multiple variable expansion procedures and applications to partial differential equations. Prerequisites: MA3132.
- **MA4620 Theory of Dynamical Systems** (4-0)
  This course provides an introduction to the theory of dynamical systems providing a basis for the analysis and design of systems in engineering and applied science. It includes the following topics: Second order linear systems; contraction mapping, existence and uniqueness of solutions; continuous dependence on initial conditions; comparison principle; Lyapunov stability theorems; LaSalle's theorem; linearization methods; nonautonomous systems; converse theorems; center manifold theorems; and stationary bifurcations of nonlinear systems. Prerequisites: MA2121.

Academic Certificate in Network Science

Program Manager

Ralucca Gera
Spanagel Hall, Room 260
(831) 656-2230
FAX (831) 656-2355
rgera@nps.edu

Brief Overview

The Academic Certificate in Network Science provides education in the use of mathematical methods for the analysis, understanding, and exploitation of complex networks. Network Science has emerged as an area critical to the success of the mission of the Navy and the Department of Defense because of the central role it plays in cyber-security, network-centric warfare, and other related areas of critical interest. A thorough understanding of the underlying mathematics is essential for the correct interpretation and further development of practical methods, models, and approaches to problems involving complex networks. The certificate program is designed to provide that very background. Upon successful completion of the coursework, students will be awarded a certificate of accomplishment in keeping with standard practices of the Naval Postgraduate School.

Requirements for Entry

Prospective students must meet the necessary prerequisites for the courses in the program.

Entry Date

Program entry dates are flexible and students who wish to pursue this certificate should coordinate with the program manager. Generally students enter start it in the Fall quarter starting with MA 3025.

Program Length

Variable, usually 1 year (1 class per quarter).

MA Academic Certificate Requirements

To earn the academic certificate students must pass all four courses with a C+ (2.3 Quality Point Rating (QPR)) or better in each course and an overall QPR of 3.0 or better. Students earning grades below these standards will need to retake the courses to bring their grades within standards or they will be withdrawn from the program.

Required Courses

- **MA3025 - Logic and Discrete Mathematics** (4-1) Offered in the Fall and Spring quarters
  MA3025 provides a rigorous foundation in logic and elementary discrete mathematics to students of mathematics and computer science. Topics from logic include modeling English propositions, propositional calculus, quantification, and elementary predicate calculus. Additional mathematical topics include elements of set theory, mathematical induction, relations and functions, and elements of number theory.
  Prerequisite: MA1025 or MA2025
- **MA4027 Graph Theory and Applications** (4-0) offered in the Fall quarters
  Advanced topics in the theory of graphs and digraphs. Topics include graph coloring, Eulerian and Hamiltonian graphs, perfect graphs, matching and covering, tournaments, and networks. Application areas with DoD/DoN relevance range from mathematics to computer science and operations research, including applications to coding theory, searching and sorting, resource allocation, and network design. Prerequisites: MA3025.
- **MA4404 Structure and Analysis of Complex Networks** (4-0) offered in the Winter quarters
  The course focuses on the emerging science of complex networks and their applications, through an introduction to techniques and models for understanding and predicting their behavior. The topics discussed will be building mainly on graph theory concepts, and they will address the mathematics of networks, their applications to the computer networks and social networks, and their use in research. The students will learn the fundamentals of dynamically evolving complex networks, study current research in the field, and apply their knowledge in the analysis of real network systems through a final project. DoD applications include security of critical communication infrastructure.
- **One of:**
  - i. **MA4400 Cooperation and Competition** (4-0) Offered in the Summer quarters
    The course will develop game theoretic concepts in evaluations of the importance of players in bargaining situations and of elements in networks. Topics covered include applications to economics, political science, and biology. There will be extensive reading from the literature. Prerequisites: MA3042, OA3201, and an introductory course
  - ii. **CS4558 Network Traffic Analysis** (3-2). Offered in the Fall quarters
    Explores fundamentals of packet-switched network traffic analysis at the network layer and above as applied to problems in traffic engineering, economics, security, etc. destination matrix estimation, application mix determination, deep-packet inspection, fingerprinting, intrusion detection and insider threat mitigation. Finally, the course co
  - iii. **OA4202 Network Flows and Graphs** (4-0) Offered in the Summer quarters
    Introduction to formulation and solution of problems involving networks, such as maximum flow, shortest route, minimum cost flows, and PERT/CPM. Elements of graph t personnel management. Prerequisite: OA3201.