

Rutgers University, Department of Electrical and Computer Engineering
ABET COURSE SYLLABUS
COURSE: 14:332:424

Course Catalog Description:	14:332:424 - Introduction to Information and Network Security (3) Classical cryptosystems, modular arithmetic, modular exponentiation, Fermat and Euler theorem, DES, modes of operation for block ciphers, breaking DES, Rijndael, public key cryptography, primality and prime testing, secret sharing schemes, Needham-Schroeder, Kerberos, public key infrastructure, password systems, information theoretic security, and applications to network security.
Pre-Requisite Courses:	14:332:226 and 14:332:312
Co-Requisite Courses:	None
Pre-Requisite by Topic:	1. Probability and Random Processes. 2. Discrete Mathematics
Textbook & Materials:	W. Trappe, <i>Introduction to Cryptography with Coding Theory</i> , 2nd Ed, Prentice Hall, 2005
References:	C. Kaufman, R. Perlman, and M. Speciner, <i>Network Security: Private Communication in a Public World</i> , 2nd Ed., Prentice Hall, 2003
Overall Educational Objective:	To provide solutions to securing the digital communication infrastructure and networks.
Course Learning Outcomes:	A student who successfully fulfills the course requirements will have demonstrated: <ol style="list-style-type: none">1. Ability to comprehend the mathematics that comprise the foundations of cryptography, including discrete mathematics and probability theory.2. An understanding of the threats and security design flaws that commonly undermine the construction of secure communication systems.3. Ability to translate mathematical principles into software implementations of basic cryptographic building blocks.4. An understanding of the different security tools that may be applied to achieve the core security objectives of confidentiality, authentication, integrity and non-repudiation.
How Course Outcomes are Assessed:	HW Problems (10 %)

Two Mid-Term Exams (40 %)
 Two Computer Projects (30 %)
 Term Project and Report (20 %)

N = none S = Supportive H = Highly Related

Outcome	Level	Proficiency assessed by
(a) an ability to apply knowledge of Mathematics, science, and engineering	H	HW Problems, Exams
(b) an ability to design and conduct experiments and interpret data	S	Computer Projects
(c) an ability to design a system, component or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability	S	Term Project and Report
(d) an ability to function as part of a multi-disciplinary team	S	Computer Project, Term Project/Report
(e) an ability to identify, formulate, and solve ECE problems	H	HW Problems, Exams
(f) an understanding of professional and ethical responsibility	N	
(g) an ability to communicate in written and oral form	H	Computer Projects, Term Project/Reports
(h) the broad education necessary to understand the impact of electrical and computer engineering solutions in a global, economic, environmental, and societal context	N	
(i) a recognition of the need for, and an ability to engage in life-long learning	S	Homework
(j) a knowledge of contemporary issues	S	Term Project/Reports
(k) an ability to use the techniques, skills, and modern engineering tools necessary for electrical and computer engineering practice	S	HW Problems, Exams
Basic disciplines in Electrical Engineering	H	HW Problems, Exams
Depth in Electrical Engineering	S	HW Problems, Exams
Basic disciplines in Computer Engineering	H	HW Problems, Exams
Depth in Computer Engineering	S	HW Problems, Exams
Laboratory equipment and software tools	H	HW Problems, Computer Projects,
Variety of instruction formats	S	Lecture, office hour discussions

Topics Covered week by week:

- Weeks 1 and 2:** Classical Cryptosystems: Shift ciphers, Affine cipher, Vigenere Cipher, One-time pads, linear feedback shift registers
- Weeks 3 and 4:** Number Theory: Modular arithmetic, Modular exponentiation, Fermat and Euler theorem
- Weeks 5 and 6:** Symmetric Encryption: A simplified DES-type algorithm, DES, Modes of operation, Breaking DES, Rijndael (AES)
- Weeks 6 and 7:** Public Key Cryptography: RSA algorithm, Primality testing, Factoring, Public Key Cryptosystems
- Weeks 7 and 8:** Digital Signatures: RSA signatures, ElGamal signatures, Hash functions (MD5 and SHA), Birthday attacks
- Weeks 9 and 10:** Secret Sharing Schemes: Secret splitting, Threshold schemes
- Weeks 11 and 12:** Key Establishment and Authentication Systems: Needham-Schroeder, Kerberos, Public Key Infrastructure, Password Systems and Unix Salt
- Weeks 13 and 14:** Information Theoretic Security: Probability, Bayes Theorem, Entropy, Conditional Entropy, Secrecy; Applications and Network Security: Networks and Routing, IPSEC, SSL/TLS, and Worm Modeling
- Weeks 15 & 16:** Review and Last Examination

Computer Usage: Matlab and Java Programming Projects

Laboratory Experiences: None

Design Experiences: None

Independent Learning Experiences: 1. Homework; 2. Computer Projects; 3. Term Project and Report

Contribution to the Professional Component:

(a) College-level mathematics and basic sciences: 0.25 credit hours

(b) Engineering Topics (Science and/or Design): 2.75 credit hours

(c) General Education: 0 credit hours

Total credits: 3

Prepared by: W. Trappe

Date: May 2011