Cryptology Course Outlines

Table of Contents

Applied Finite Mathematics

Course Description

Course: MATH 261 Applied Finite Mathematics
Credits: 3
Prerequisite: MATH 143, MATH 144, MATH 145, or MATH 153 with a C− or higher, or placement test.
Course Description: Number systems, integer rings, finite fields, number theory algorithms, prime numbers and primality tests, factoring, and random numbers.

Course Objectives

After completing this course the student should have the following competencies:

1. an understanding of binary, octal, and hexadecimal numbers;
2. an understanding of integer rings and finite fields;
3. the ability to use the Euclidean algorithm, the Chinese remainder theorem, Euler's ϕ function, Fermat's little theorem, and Euler's theorem;
4. an understanding of the different methods that can be used to find prime numbers;
5. an understanding of factoring algorithms and their uses;
6. an understanding of the processes used to generate random numbers.

Course Outline

1. Number systems
   - Representations of numbers
   - Binary, octal, and hexadecimal numbers
2. Modular arithmetic
3. Integer rings
4. Finite fields
   - Galois fields
   - Extension fields
5. Euclidean and extended Euclidean algorithms
6. Chinese remainder theorem
7. Euler's ϕ function
8. Fermat's little theorem
9. Euler's theorem
10. Prime numbers
    - Finding prime numbers: Sieve of Erastothenes etc.
    - Primality tests
11. Factoring
    - Divisibility and unique factorization

    - Factoring algorithms
12. Random numbers
    - Random and psuedorandom number generators

Bibliography

1. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Third Edition*, Chapman & Hall/CRC Cryptography and Network Security Series. CRC Press, 2021.
2. Margaret Cozzens and Steven Miller. *The Mathematics of Encryption: An Elementary Introduction.* Mathematical World, V. 29. American Mathematical Society, 2013.
3. Samuel Wagstaff. *The Joy of Factoring.* Student Mathematical Library, V. 68. American Mathematical Society, 2013.
4. Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners.* Springer, 2010.
5. Eric Gossett. *Discrete Mathematics with Proof, Second Edition.* Wiley, 2009.
6. Jeffrey Hoffstien, Jill Pipher, and Joseph Silverman. *An Introduction to Mathematical Cryptography.* Springer, 2008.
7. Shafi Goldwasser and Mihir Bellare. *Lecture Notes on Cryptography.* Available at https://cseweb.ucsd.edu/~mihir/papers/gb.pdf, 2008.
8. Albrecht Beutelspacher. *Cryptology.* Mathematical Association of America, 1994.

Applied Cryptography

Course Description

Course: MATH 361 Applied Cryptography
Credits: 3
Prerequisite: A grade of C or better in MATH 261 Applied Finite Mathematics.
Course Description: Symmetric cryptography, modular arithmetic, stream and block ciphers, random numbers, Advanced Encryption Standard, public-key cryptography, key exchange, digital signatures, hash functions, message authentication.

Course Objectives

After completing this course the student should have the following competencies:

1. an understanding of the basic concepts of symmetric cryptography including symmetric keys, cleartext, ciphertext, and simple encryption methods such as the replacement cipher;
2. an understanding of the basic concepts of cryptanalysis and the methods used to attack an encryption system;
3. the ability to do computations in a ring of integers modulo n and an understanding of ciphers that use such rings;
4. an understanding of simple stream ciphers;
5. an understanding of the different types of random number generators that are used in cryptography and the ability to use random number generators to create ciphers such as a one-time pad;
6. an understanding of the important modes of operation for block ciphers;
7. a basic understanding of Galois fields and the ability to do computations in $GF(p^n)$;
8. an understanding of the structure of the Advanced Encryption Standard (AES) and the ability to encrypt and decrypt messages using the AES;
9. an understanding of the principles and common applications of public-key cryptography, and the primary number theory used in public-key cryptography;
10. an understanding of the RSA cryptosystem, the mathematics used in the system, and the ability to encrypt and decrypt cleartext using the system;
11. an understanding of the Diffie-Hellman key exchange and its applications;
12. an understanding of the basic digital signature protocol and the ability to use the RSA signature scheme;
13. an understanding of the purpose, security requirements, and properties of hash functions and the ability to use common hash function algorithms;
14. an understanding of the properties of message authentication codes and the ability to use hash functions to build a message authentication code.

Course Outline

1. Basics of cryptography
2. Symmetric encryption
   - Replacement cipher
3. Basic cryptanalysis
4. Modular arithmetic
   - The ring of integers modulo n
5. Stream ciphers
6. Random numbers
   - Random number generators
   - The one-time pad
7. Encryption using block ciphers
   - Modes of operation
8. The Advanced Encryption Standard (AES)
   - Galois fields
   - Structure of the AES
   - AES decryption
9. Public-key cryptography
   - Principles
   - One-way functions
   - Applications: key establishment, nonrepudiation, identification, encryption
   - The Euclidean and extended Euclidean algorithms
   - Euler's ϕ function
   - Fermat's little theorem and Euler's theorem
10. The RSA cryptosystem
11. Key exchange
    - Diffie-Hellman key exchange
    - Basic group theory (cyclic groups and their subgroups) (optional)
    - The discrete logarithm problem (optional)
    - Security of Diffie-Hellman key exchange (optional)
12. Digital signatures
    - Basic digital signature protocol
    - The RSA signature scheme
13. Hash functions
    - The purpose of hash functions
    - Hash function security requirements and properties
    - Hash function algorithms
14. Message authentication
    - Properties of message authentication codes
    - Building a message authentication code from a hash function

Bibliography

1. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Third Edition*, Chapman & Hall/CRC Cryptography and Network Security Series. CRC Press, 2021.
2. J Vacca. *Computer and Information Security Handbook, 2nd Edition*. Elsevier, 2013.
3. Margaret Cozzens and Steven Miller. *The Mathematics of Encryption: An Elementary Introduction*. Mathematical World, V. 29. American Mathematical Society, 2013.
4. Samuel Wagstaff. *The Joy of Factoring*. Student Mathematical Library, V. 68. American Mathematical Society, 2013.
5. Alasdair McAndrew. *Introduction to Cryptography with Open-Source Software*, Discrete Mathematics and its Applications series. CRC Press, 2011
6. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley, 2010.
7. Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.
8. Jeffrey Hoffstien, Jill Pipher, and Joseph Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.
9. Shafi Goldwasser and Mihir Bellare. *Lecture Notes on Cryptography*. Available at https://cseweb.ucsd.edu/~mihir/papers/gb.pdf, 2008.
10. Niels Ferguson. *Practical Cryptography*. Wiley, 2003.
11. Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Second Edition, 1996.
12. Albrecht Beutelspacher. *Cryptology*. Mathematical Association of America, 1994.

Applied Cryptanalysis

Course Description

Course: MATH 461 Applied Cryptanalysis
Credits: 3
Prerequisite: MATH 361 Applied Cryptography with a grade of C or better
Course Description: Cryptanalysis concepts; cryptanalysis of symmetric and public key cryptosystems, key exchange systems, and digital signatures; hash function collision resistance; cryptanalysis with quantum computers.

Course Objectives

After completing this course the student should have the following competencies:

1. an understanding of the basic concepts of cryptanalysis and the methods used to attack an encryption system;
2. the ability to implement an exhaustive key search against a symmetric cryptosystem;
3. an understanding of basic factoring algorithms and the ability to use those algorithms;
4. an understanding of how to attack the RSA cryptosystem using a factoring algorithm;
5. an understanding of how to find a brute force solution to the discrete logarithm problem, and the ability to conduct a man-in-the-middle attack against the Diffie-Hellman key exchange;
6. an understanding of how to attack the RSA signature scheme;
7. an understanding of the concept of collision resistance and The Birthday Attack;
8. an understanding of what the development of quantum computers will mean to the security of public key cryptography.

Course Outline

1. General mathematical cryptanalysis concepts
    - Key recovery vs. decryption
    - Kerckhoffs' Principle
2. Cryptanalysis of symmetric cryptosystems
    - Symmetric cryptosystems
    - Brute force attacks
        - Exhaustive key search
        - Key lengths and security levels
3. Public key cryptography review
4. Review of the RSA cryptosystem
5. Factoring algorithms
6. Mathematical attacks on RSA
    - Preventing mathematical attacks

7. Key exchange
    - Review of the Diffie-Hellman key exchange
    - The discrete logarithm problem
        - Brute force solutions
    - The generalized Diffie-Hellman problem
    - Man-in-the-middle attack against the Diffie-Hellman key exchange
8. Digital signatures
    - Review of the principles of digital signatures
    - Review of the RSA signature scheme
    - Attacks against the RSA signature scheme
9. Hash functions
    - Collision resistance
    - The Birthday Attack
10. Implications of quantum computers on public key cryptography

Bibliography

1. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Third Edition*, Chapman & Hall/CRC Cryptography and Network Security Series. CRC Press, 2021.
2. J Vacca. *Computer and Information Security Handbook, 2nd Edition*. Elsevier, 2013.
3. Margaret Cozzens and Steven Miller. *The Mathematics of Encryption: An Elementary Introduction*. Mathematical World, V. 29. American Mathematical Society, 2013.
4. Samuel Wagstaff. *The Joy of Factoring*. Student Mathematical Library, V. 68. American Mathematical Society, 2013.
5. Alasdair McAndrew. *Introduction to Cryptography with Open-Source Software*, Discrete Mathematics and its Applications series. CRC Press, 2011
6. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications*. Wiley, 2010.
7. Christof Paar and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.
8. M. Jason Hinek. *Cryptanalysis of RSA and Its Variants*, Cryptography and Network Security Series. Chapman & Hall/CRC, 2009.
9. Antoine Joux. *Algorithmic Cryptanalysis*, Cryptography and Network Security Series. Chapman and Hall/CRC, 2009.
10. Christopher Swenson. *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. Wiley, 2008.
11. Jeffrey Hoffstien, Jill Pipher, and Joseph Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2008.
12. Shafi Goldwasser and Mihir Bellare. *Lecture Notes on Cryptography*. Available at https://cseweb.ucsd.edu/~mihir/papers/gb.pdf, 2008.
13. Niels Ferguson. *Practical Cryptography*. Wiley, 2003.
14. Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Second Edition, 1996.
15. Albrecht Beutelspacher. *Cryptology*. Mathematical Association of America, 1994.