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.