Applied Cryptography

Table of Contents

1 Course Description

Course: 2030:361 Applied Cryptography
Credits: 3
Prerequisite: A grade of C- or better in either 2030:154 Technical Mathematics IV or 2030:216 Applied Finite Mathematics
Bulletin Description: Prerequisite: A grade of C- or better in either 2030:154 or 2030:216. Symmetric cryptography, modular arithmetic, stream and block ciphers, random numbers, Advanced Encryption Standard, public-key cryptography, key exchange, digital signatures, hash functions, message authentication.

2 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.

3 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

4 Bibliography

1. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, 2nd Edition*, Chapman \ Hall/CRC Cryptography and Network Security Series. Chapman and Hall/CRC, 2014.
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 http://cseweb.ucsd.edu/~mihir/papers/gb.html, 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.