Applied Cryptography

Course Description

Course: 2030:361 Applied Cryptography  
Credits: 3  
Prerequisite: A grade of C or better in 2030:216 Applied Finite Mathematics.  
Bulletin Description: Prerequisite: A grade of C or better in 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.

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 \( \phi \) 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