Prof. Dr. Fahreddin M. Sadıkoglu

Computer Engineering Department

COM 457-Cryptography and Coding Theory

Course Description:

Introduction to Cryptography. Terminology. Importance of Security. Security Attack. Security Mechanism: Confidentiality, Integrity and Authentication. Symmetric-Key and Public-Key Encryptions. Classical Encryption Techniques: Shift Cipher, Substitution Cipher, Affine Cipher, Vigenere Cipher, Hill Cipher. Introduction to Number Theory. Modular Arithmetic. Discrete Logarithm DES, RSA Algorithms. Hash Functions. Key Establishment Protocols. Authentication and Digital Signature Protocols. Secure Electronic Transactions. Error Correcting codes. Computer Problems Using MATLAB.

Course Objectives: At the end of the course the student will understand:

- Classical Cryptosystems
- DES - Data Encryption Standard
- AES (Rijndael) - Advanced Encryption Standard
- SHS - Secure Hash Algorithm and Standard
- RSA - Public Key Algorithms
- Elleptic Curve Cryptography
- Diffie Hellman Key Exchange
- Authentication and Digital Signature Principles
- E-Commerce and Digital Cash
- Error Correcting Codes

Course Grade Determination:

Grade=15%(Homework)+15%(Laboratory) + 30%(Midterm)+ 40(Final Exam)

Text Book:

1. Wade T., Lawrence C. Cryptography with Coding Theory. Prentice-Hall, NJ,2002

Reference Books:

2. Stallings William. *Cryptography and network Security: Principle and Practice*. Prentice-Hall, NJ,1999

3. Menezes et all. *Handbook of Applied Cryptography*. CRC Press, FL,1997

4. Stallings W. *Network Security Essentials. Applications and Standards.* Prentice-Hall, NJ, 2000

5. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed.New York: John Wiley & Sons, 1996

6. Stinson, D. R. *Cryptography: Theory and Practice*. 2nd Edition Boca Raton, FL: CRC Press, 2002

Weekly Schedule

Week	Subject	References
1	Secure Communications. Security Attacks.Introduction to Symmetric and Public Key Algoritims. Block and Stream Ciphers. Cryptography Applications.Exercises, Computer Problems.	[1], pp.1-9 [2], pp.4-14
2	Classical Cryptography Shıft Cipler. Frequency Distribution of English Letters. Affine Ciphers. Viegener Ciphers.Exercises, Computer Problems.	[1], pp.12-16 [2], pp.24-47
3	The Playfair and ADFGX Ciplers. Hill Ciphers. Substitution and Tranposition Techniques. Exercises, Computer Problems.	[1], pp.23-29 [2], pp.24-47
4	Basic Number Theory. Prime Member. Congruences. Chinese Remainder Theorem. Primitive Root. Square Root Modul on. Exercises, Computer Problems.	[1], pp.59-81 [2], pp.107-115 236-245
5	DEC. Differential Cryptoanalysis. Breaking DEC. Triple DEC. Blowfish. RC5. Exercises, Computer Problems.	[1], pp.97-118 [2], pp.56-98 174-198
6	Public Key Cryptography. Rijndael. RSA. Exercises, Computer Problems.	[1], pp.127-159 [2], pp.259-278
7	Primarity Testing. Factoring. Discrete Logarithms.Exercises, Computer Problems.	[1], pp.165-176 [2], pp.245-252
8	Digital Signatures. RSA Elgamal Signatures. Probabilistic Signature.Exercises, Computer Problems.	[1], pp.177-189 [2], pp.380-395
9	Mesage Authentication. MAC Hash Functions. Exercises, Computer Problems.	[1], pp.182-191 [2], pp.312-335 348-372
10	Secure Electronic Transactions. E-Commera And Digital Cash.Exercises, Computer Problems.	[1], pp.177-199 [2], pp.548-560
11	Key Establishment Protocols. Diffile Hellman Key Exchange. Kerberos.Exercises, Computer Problems.	[1], pp.236-246 [2], pp.286-293
12	Elleptic Curve Cryptography.Introduction To Quantum Cryptography and DNA Computing.Exercises, Computer Problems.	[1], pp.272-290 354-370 [2], pp. 297-304
13	Error Correcting Codes.Hamming Code. Linear Code Confvolution Codes. Colay Codes. Exercises, Computer Problems.	[1], pp.295-329
14	Cyclic Codes. BCH Codes.Reed Solomon Codes. Exercises, Computer Problems.	[1], pp.329-345