CST466/CST366 – Cryptography

Syllabus for Spring 2009, Section 24

Instructor: Jim Kenevan
Office: 600H Schaumburg
Phone: 847-619-8491
Email: jkenevan@roosevelt.edu

Office Hours:
4:00-6:00 Monday Gage
4:00-6:30 Tuesday Schaumburg 600H

Class:
Time: 6:30-9:00 PM Tuesday
Room: Sch 334

Topics

• History
  o Ancient
  o Primitive codes
  o Secret inks
  o Black chambers, including American and Yardley
  o Civil war, Crimean war, WWI and WW2
  o Specific encryption machines and decryption machines
    ▪ Ceasar
    ▪ Enigma
    ▪ Colosus
    ▪ M-131
    ▪ Sigsaly
  o Soviet

• Popular ciphers
• DEA – Data Encryption Standard
• AEA – Advanced Encryption Standard
• Public Key Encryption
• Other encryption methods
• Numbers radio stations
• An introduction to decryption
• Intrusion detection
Software Projects

We will code three major projects
1. DES
2. AES
3. Public key

Grading

Projects will be 40%, homework 20%, midterm 20%, and final 20%.

Policy on Cheating

I expect students to help one another, but each student should produce his own work. For example, you can show a friend your code, but you must not “give” the code away, nor should a student copy and reproduce that code for credit.

Cheating will result in a lower course grade.