

CS 6623 Data Security

Fall 2007, Credit Hrs: 3

General Information

Instructor: Hai Jiang
Office: CSM, Room 127
Phone: 972-3978 ext. 118
Email: hjiang@cs.astate.edu

Time: Tue Thu 12:30 - 1:45 p.m.

Location: CSM, Room 212

Office Hours: Tue Thu 10:45 a.m. - 12:30 p.m. & 1:45-2:45 p.m.

Syllabus: <http://www.csm.astate.edu/~hjiang/cs6623/syllabus.pdf>

Course Homepage: <http://www.csm.astate.edu/~hjiang/cs6623.html>
(Lecture notes, homework assignments, etc.)

Course Description

This course is designed to cover the basic issues and principles of cryptographic and network security techniques. The course consists of three parts: mathematical background, cryptography, and network security. The first part (mathematical background) introduces the principle of number theory and some results from probability theory, including Primes, random numbers, modular arithmetic and discrete logarithms. The second part (cryptography) covers cryptographic algorithms and design principles, including conventional and symmetric encryption (DES, IDEA, Blowfish, Rijndael, RC-4, RC-5), public key or asymmetric encryption (RSA, Diffie-Hellman), key management, hash functions (MD5, SHA-1, RIPEMD-160, HMAC), digital signatures, and certificates. The third part (network security) deals with practical applications that have been implemented and are in use to provide network security, including authentication protocols (X.509, Kerberos), electronic mail security (S/MIME, PGP), web security and protocols for secure electronic commerce (IPSec, SSL, TLS, SET).

Course Objectives

At the end of the course, students should understand:

- DES - Data Encryption Standard
- AES (Rijndael) - Advanced Encryption Standard
- RC4 - Stream Cipher
- MD4, MD5 - Message Digest Algorithms
- SHS - Secure Hash Algorithm and Standard
- RSA - Public Key Algorithms
- Diffie Hellman - Key Exchange
- Authentication Systems for people and Computers

- Kerberos
- Electronic Mail Security
 - S/MIME - Secure/Multipurpose Internet Mail Extension
 - PGP - Pretty Good Privacy
- IP and Web Security
 - SSL - Secure Sockets Layer
 - TLS - Transport Layer Security
- Concepts of Digital Watermarking and Steganography

Textbook

- William Stallings, *Cryptography and Network Security: Principles and Practice*, 4th edition, Prentice Hall, 2005, 646 pages, ISBN: 0131873164.

References

- Richard J. Spillman, **Classical and Contemporary Cryptology**, Prentice Hall, 2004, 304 pages, ISBN: 0131828312.
- Bruce Schneier, **Applied Cryptography: Protocols, Algorithms, and Source Code in C**, 2nd edition, Wiley, 1995, 784 pages, ISBN 0471117099.
- More course materials will be available on course homepage. Please visit it often for changes and announcements.

Grading

Final grades will be calculated based on the following weights:

Homework and Programming Assignments:	20%
Midterm Exam:	20%
Project:	20%
Presentation:	10%
Final Exam:	30%

The final grade will be distributed as :

A	[90-100]
B	[80 - 90)
C	[70 - 80)
D	[60 - 70)
F	[0 - 60)

Policies

Food and Drinks

Department policy restricts bringing either food or drinks into the classroom.

Electronic Devices

Cell phones are restricted during class. Cell phones must be turned off during the lecture. If your cell phone rings during class, you may be asked to leave. Other devices (computers, recorders, etc.) may be allowed, but you must ask the instructor before you use them during class.

Special Facilities

Students who require academic adjustments in the classroom due to a disability must first register with ASU Disability Services. Following registration and within the first two weeks of class, please contact the instructor to discuss the appropriate academic accommodations to ensure equal access to this course.

Rescheduling Tests

Tests cannot be rescheduled due to testing in other classes. If a test is missed due to extenuating circumstances then you must notify me as soon as possible. The circumstances must be documented by you and must be excusable in order to reschedule a test.

Late Assignments

For most homework assignments, the class will receive a working solution within four days after the due date. *NO* assignments will be accepted that are more than four days late. Assignments that are less than a week late, will be accepted with certain penalty (25% per day).

Cheating

You are encouraged to discuss problems and programming assignments with each other. Helping others learn is often the most powerful way of mastering material yourself. However, taking somebody else's solution without their knowledge or consent is cheating and will be punished. Do not leave copies of the programming assignments in the trash can in a public place -- throw them away at home or some other private place. Also do not leave your directories unprotected. There are harsh penalties for those found cheating.

Attendance

Attendance is required. If you miss a class, you are responsible for material covered during the class you missed, this includes any assignments made. Note that I do not provide one-on-one instruction for missed classes.