

CS 6520-01 Cryptography and Data Security
Winter 2008
MWF 10:40–11:50 a.m., Sc S 125

Instructor: William R. Nico

Office: Robinson Hall 239

Phone: (510)885-3386

E-mail: nico@csueastbay.edu (On the mcs system just “nico” will work.)

Web: www.mcs.csueastbay.edu/~nico

Office hours: MW 1:00–2:30 p.m. or by appointment

Text: William Stallings, *Cryptography and Network Security Principles and Practice*, Fourth Edition, Prentice Hall, 2006.

Recommended: B. Schneier, *Applied Cryptography*, Second Edition, John Wiley, 1995.

This course will deal with the basic problems of data security including privacy, integrity, and authenticity. Cryptography and cryptographic protocols play a central role in dealing with these problems. Topics to be covered include:

- Mathematical background for cryptography (probability, information theory, modular arithmetic, finite fields, computational complexity)
- Cryptographic algorithms (ciphers vs. codes, stream vs. block ciphers, transposition systems, symmetric vs. asymmetric algorithms including DES, AES, RSA, and others)
- Cryptographic systems (key management, digital signatures, passwords)
- Access and information-flow control, including standards such as TCSEC and the Common Criteria
- Related topics (if time allows), such as inference control in statistical databases, and interactive proof systems with applications to authentication.

The exact time allotted to various topics will depend on the background and interest of the class.

There will be regular written homework, a mid-term exam, a final exam, and an extended review of a recent research paper (whether this will be written or oral will depend, in part, on the preference of the class); the paper will be chosen from the published research literature by mutual agreement between the student and instructor.

Grading: The course grade will be computed roughly as follows. (The date of the midterm is subject to change. Any change will be announced in class.)

- | | |
|------------------------------------------------------------|-----|
| 1. Final exam (Wednesday, March 19, 11:00 a.m.–12:50 p.m.) | 50% |
| 2. Midterm (Wednesday, February 6) | 30% |
| 3. Homework (as assigned) | 10% |
| 4. Paper/presentation (no later than Wednesday, March 12) | 10% |

Late homework will *not* be accepted. Homework is to be turned in at the *beginning* of class on the due date. Homework is to represent *individual* efforts! Any work not your own, e.g., results obtained from reference sources, should receive appropriate bibliographic *citations*. *Plagiarism* will be subject to appropriate penalties, as described under *Academic Dishonesty* in the catalog.

Written work: Any written work submitted for the course, *including in-class tests*, must be done in *ink*!

Make-up policy: Make-up tests will be considered only in *unusual* circumstances, and then only if arrangements have been made in *advance*.