DEPARTMENT OF MATHEMATICS
California State University, Bakersfield
MATH 477 – Applied Cryptography

Instructor: Charles Lam
Office: SCI 114E
Phone: (661) 664 2403
Email: clam@csub.edu
Homepage: http://www.csub.edu/∼clam

Class times: 3:30-5:30M (SCI 176), 3:30-5:30TR (DDH 107E)

Office Hours: 10-11:30MTR, 1-2M, or drop by when I am in.

Course Description/Objectives: An introduction to cryptography, history and its present day use. Topics include symmetric ciphers, hash functions, data integrity, public-key encryption, digital signatures, key establishment, key management. Related topics such as prime generation, integer factorization, discrete logarithms, pseudo-random number generation and computational complexity will also be discussed.

Text: Introduction to Cryptography with Coding Theory, Second Edition, by W. Trappe and L.C. Washington

Web page: The web page for the course is at http://www.csub.edu/∼clam/math477w06.html

Labs: You are required to work in groups of 2-4 on assigned problems and hand in the lab reports **individually** a week after.

Grading: In addition to labs and homework, there will be one midterm test, one take-home final exam, and a project.

Labs	20%
Homework	20%
Project	25%
Midterm	15%
Final Exam	20%