DEPARTMENT OF MATHEMATICS
California State University, Bakersfield
MATH 475 – Applied Cryptography

Instructor: Charles Lam
Office: SCI-3 209 / SCI 1-101
Phone: (661) 654 2403 / (661) 654 3450
Email: clam@csub.edu
Homepage: http://www.csub.edu/∼clam

Class times: TR 5:10pm-7:30pm (SCI 3-103)

Office Hours: M 4-5, TR 3-5 or drop by when I am in.

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

Course Goals:

(1) Understand the use of cryptography in practical applications relating to information security.
(2) Understand the mathematics behind cryptographic primitives.

Text: Understanding Cryptography: A Textbook for Students and Practitioners, by C. Paar, J. Pelzl, 978-3642041006

Topics covered: Whole text, if time permits.

Web page: The web page for the course is at http://www.csub.edu/∼clam/math475f14.html

Student Activity: There will be some problem solving work in each class, based on materials taught. Attendence is required.

Homework: Homework will be given every week. Points will be assigned to each problem. Students are expected to hand in homework in a timely manner, and no later than the 9th week of classes. Homework will be graded on a basis of “Accept” or “re-do”. You are required to accumulate at least 200 points of “Accept” to receive full credit of the homework component.

Homework Presentations: Every Monday, students are required to take turns to present homework solutions.

Presentation:
Grading: In addition to presentations, quizzes and homework, there will be one test, and a final exam (cumulative). A pass (50%) in the final exam is required to obtain a final grade of D- or better.

Homework	30%
Student Activity	5%
Midterm	20%
Project Presentation .	20%
Final Exam	25%

Test Dates:

- Midterm: October 21, Tuesday (tentative)
- Final Exam: November 25, Tuesday, 5-7:30pm

Remarks:

- There will be no make-up exams or tests. If you know in advance that you are going to miss an exam, please make your arrangements with me at least one week ahead.
- Please hand in labs and homework on time. Late labs and homework will be accepted up to the beginning of next class for 50% of credit.

Academic Dishonesty:

You are encouraged to work with your classmates in labs and homework. However, YOU ARE REQUIRED TO HAND IN WORK WRITTEN BY YOURSELF. A rule of thumb is to destroy any evidence of discussion before writing up the solutions yourself.

If you collaborated with anyone, ACKNOWLEDGE COLLABORATORS. Please also note that, ACKNOWLEDGING YOUR FRIENDS ON THE CONTRIBUTION DOES NOT MEAN YOU HAVE THE RIGHT TO COPY OTHERS' WORK. YOU MUST WRITE THE SOLUTIONS IN YOUR OWN WORDS.

If you are caught cheating, the policy for this class is -10% to the final grade on the first offense, -20% for the second, and -50% thereafter.