CSCI 663 Introduction to Cryptography

Course Description:
This course considers the basic knowledge of cryptography and its application, both traditional and modern. This knowledge is the basis for future studies on network security.

Prerequisites
CSCI 369 Java Programming, and MATH 234 Analytic Geometry and Calculus I

Course Objective The learner will...
- understand security goals and attacks upon security.
- be able to apply both traditional and modern symmetric-key ciphers.
- explore the Data Encryption Standard and Advanced Encryption Standard.
- apply encipherment using modern symmetric-key ciphers.
- learn asymmetric-key cryptography.
- apply the basic mathematics of cryptography (not including proof).

Background:
Cryptography is the science of designing algorithms and protocols that guarantee privacy, authenticity, and integrity of data when parties are communicating or computing in an insecure environment. The recent explosion of electronic communication and commerce has expanded the significance of cryptography far beyond its historical military role into all of our daily lives. For instance, cryptography provides the technology that allows us to use our credit card to make on-line purchases without allowing others on the internet to learn our credit card number.

Course Text
Behrouz A. Forouzan
Cryptography and Network Security
McGraw-Hill, copyright @ 2008
ISBN 978-0-07-287022-0
This course covers Chapter 1, 3, 5, 6, 7, 8 and 10. Chapters 2, 4, and 9 review mathematical foundation. We introduce this material in general as needed.

Methods of Instruction
Instructional methods will include lectures, class discussions, programming projects, and assignments.

Methods of Evaluation for Undergraduates:
Course requirements will include class participation, programming projects, assignments, and tests. The percentage is allocated as follows:
- Three Programming Projects: 30%
- Seven Homework Assignments: 28%
- Midterm Test: 12%
- Final Test: 25%
Participation: 5%

**Methods of Evaluation for Graduate Students:**
There will be more evaluation methods for graduate students. Course requirements will include programming projects, research paper and presentations, teaching, assignments, and tests (both paper and oral). The percentage is allocated as follows:

- Three Programming Projects: 18%
- Seven Homework Assignments: 21%
- Teaching One Class Session: 10%
- One Research Paper and Presentation: 25%
- Midterm Test (paper only): 9%
- Final Test (paper and oral): 17%

For both graduate and undergraduate students, the grade cuts are 90%, 80%, 70%, 60%, below 60% for A, B, C, D and U respectively.

**Class Policies:**
- **General:** The student is responsible for doing all assigned readings and grasping all the material presented in class which may or may not originate from the textbook. The student will be responsible for the material covered in the lectures, assigned textbook readings and other reading assignments whether or not covered in the class lectures. To maximize your understanding, please **read the chapter before the class** in which the material will be covered.
- **Attendance:** Students are expected to attend all classes regularly and on-time. Because course requirements include in-class assignments and class participation, your grade depends to some extent on class attendance. Attendance will be taken with a sign-in sheet, so be sure to sign in each week. When you miss a class, you are responsible for getting notes and assignments from instructor, another class member or online.
- **Assignments:** Assignments and Projects are due at the beginning of class or on the assigned due date. Assignments may be turned in digital drop box. **Late assignments should be turned in as soon as possible, but will be assessed a late penalty of 10% of grade for each week late.**
- **Tests:** Special arrangements may be made to take tests early by appointment with the teacher under very extreme cases. Make-up exams are given only in extreme cases and if arrangements are made prior to the scheduled exam. **Leaving a message is not making arrangements. Make-up exams may differ in format, content, and level of difficulty** and must be completed within one week of the regularly scheduled exam.
- **Academic honesty policy:** Students are reminded of Fort Hays State University's Academic Honesty Policy, which applies to this course. The Academic Honesty Policy is printed in the University Catalog and is available online (at http://web.fhsu.edu/universitycatalog/gen/academichonesty.asp). Cheating and/or plagiarism will be punished at a minimum by a grade of zero on the work, and the case will be referred to the Office of Student Affairs for further action.
• **Special needs policy:** If you have a disability or special need, please contact the instructor. Every reasonable accommodation will be made so that any qualified student can participate in the course.

# Tentative Schedule (16 Weeks)

<table>
<thead>
<tr>
<th>Week</th>
<th>Lecture Topic</th>
<th>Assignments, Projects, Presentations, and Tests</th>
</tr>
</thead>
</table>
| Week 1 | Survey, Syllabus  
Chapter 1: Introduction  
Some math background from chapter 2 | Assignment 1 Assigned  
Grads’ Research Paper Assigned |
| Week 2 | Chapter 3: Traditional Symmetric-Key Ciphers | Assignment 1 Due  
Project 1 Assigned |
| Week 3 | Chapter 3 Continued  
Some math background from chapter 4 | Assignment 2 Assigned |
| Week 4 | Chapter 5: Introduction to Modern Symmetric-Key Ciphers | Assignment 2 Due  
Assignment 3 Assigned |
| Week 5 | Chapter 5 Continued | Project 1 Due |
| Week 6 | Chapter 6: Data Encryption Standard (DES)  
(One session will be taught by Grads) | Assignment 3 Due  
Project 2 Assigned  
Assignment 4 Assigned |
| Week 7 | Chapter 6 Continued  
Midterm Review Questions Handout | Grads Report the Progress of Their Research |
| Week 8 | Catch up Schedule  
Midterm (In Class, closed Books and Notes) | Assignment 4 Due |
| Week 9 | Chapter 7: Advanced Encryption Standard (AES) | Assignment 5 Assigned |
| Week 10 | Chapter 7 Continued | Project 2 Due |
| Week 11 | Chapter 8: Encipherment Using Modern Symmetric-Key Ciphers | Assignment 5 Due  
Assignment 6 Assigned |
| Week 12 | Chapter 8 Continued  
(One Session will be taught by Grads) | Project 3 Assigned |
| Week 13 | Some math background from Chapter 9 | Assignment 6 Due |
| Week 14 | Chapter 10: Asymmetric-Key Cryptograph | Assignment 7 Assigned |
| Week 15 | Chapter 10 Continued  
Grads Present Their Research Papers  
Final Review Questions handout | Grads’ Research Paper Due |
| Week 16 | Final Oral Test for Grads  
Final Paper Test (In class, closed book and notes) | Assignment 7 Due  
Project 3 Due |

• **This schedule is tentative and subject to change**  
• **If there are more than two graduate students in the class, then several graduate students may need to share one session’s teaching.**