Cryptology

Instructor: Dr. Ianna West

Office: Peltier 106-B

Office Hours: For immediate online consultation: Monday & Wednesday 9:00 AM – 11:00 AM and Friday 9:00 AM – 10:00 AM unless otherwise specified. To fulfill the University requirement, I am also generally in my Nicholls on-site office on Tuesday and Thursday from 9:00 AM – 1:30 PM and 3:30 PM – 4:30 PM. If you wish, you may reach me by phone or by email during those hours.

The instructor will also be available for consultation via email outside of regularly scheduled office hours. The instructor will reply to emails within 24 hours Monday through Friday. In addition, instructor will be available to answer questions on some weekends and holidays. Student may make an appointment to speak with the instructor by phone or online by Skype or Adobe Connect.

Email: ianna.west@nicholls.edu
Office Phone: 985-448-4394
Moodle: http://moodle.nicholls.edu/moodle/

Section: WWW
Location: Online

MATH 590. Topics in Graduate Mathematics. 3-3-0. Prerequisite: Permission of department head. Selected current topics in mathematics. May be repeated for credit if content differs. No student may apply more than six hours toward graduation. (27.0101)

Course Description: In this course, we will discuss the mathematics and protocols needed to make data transmission and electronic systems secure applying techniques used to protect data. These techniques belong to the field of cryptography. The terms cryptography, cryptology, and cryptanalysis are frequently interchanged and used in discussions involving secure communications and related problems. Cryptology encompasses two fields, cryptography and cryptanalysis. Cryptography is the process of designing systems to keep messages secret. Cryptanalysis deals with breaking such systems. We will define and explain cryptologic terms, concepts, and principles. We will cover classical cryptosystem and cryptanalytic techniques. We will discuss the successes and failures in cryptologic methods from both historical and modern points of views. We will discuss both symmetric key and public key encryption/decryption methods. We will discuss the one-time pad method which is unbreakable. We will describe block ciphers and stream ciphers, modes of operation of symmetric ciphers and the applications of these. More recent applications of cryptography will be discussed including the differences between authentication and non-repudiation applications.

Student Outcome Objectives:
Students will be able to:
1. Define and/or explain cryptologic terms, concepts, and principles.
2. Implement various classical cryptographic techniques by encrypting and decrypting messages.
3. Analyze authentication and key agreement protocols to identify the strengths and weaknesses.
4. Identify cryptosystems that will support the security of financial institutions and other types of institutions, for example, password protection, authentication, communication, confidentiality, password protection, etc.
5. Analyze and implement key control algorithms.
6. Analyze and implement the RSA Algorithm.
7. Determine the role of cryptography in developing more secure systems and assessing the security in current systems.
Course Hardware and Software Requirements

Access to a computer with internet is required. Students must have knowledge of the internet, including how to access a given website. Students must be able to use different components of the Moodle learning management system (LMS) including uploading a file. Students must know how to use a word processor such as Microsoft Word or a scanner to submit assignments (Word documents are preferred). Handwritten, scanned assignments must be legible once received by the instructor. If the handwritten assignments are not legible, the student will be required to use Microsoft Word or some other word processor to type the assignment. If a word processor other than Microsoft Word is used, the assignment must be submitted in pdf format, and the mathematical equations, expressions, symbols, etc. must be legible.

The student must know how to receive and send emails properly, as well as reply to an email using their Nicholls’ email account. The instructor will provide instructions on how the student must properly label and use emails in communication. Student must be able to open a pdf file using Acrobat Reader or some other pdf reader which may be downloaded free from the internet. If the students are not familiar with one or more of the software and/or web-based tools mentioned, students must have the ability to familiarize themselves with these necessary web-based tools and/or software either by exploration or tutorials. The links to important tutorials are given below.

The URL for the university’s distance learning website is http://www.nicholls.edu/distance/.

FAQS about internet courses can be viewed at the website http://www.nicholls.edu/distance/faqs/.

The FAQS website will give students insight as to what they should expect from an online course, as well as answer many frequently asked questions.

A Moodle Tutorial can be viewed at the website http://www.nicholls.edu/distance/moodle-tutorial/.

Course Content, Methods of Evaluation and Point Distribution

On-Campus Meeting or Proctor Requirements: Students will meet on-campus to take the final exam if they live within a reasonable driving distance of the campus. Distance learners must locate an approved testing facility near their home. A list of approved testing centers is given on the Proctor Approval form. There is a link to the Proctor Approval form on the Course Homepage on Moodle.

Proctor Requirements: Distance learners are those students who must take the final exam off-campus because they do not live in driving distance of Nicholls’ campus. Distance learners must locate an approved testing facility near their home. A student wishing to take the exam off-campus must inform the instructor via email and complete a Proctor Approval form which can be found on the Course Homepage on Moodle. The completed Proctor Approval form must be unloaded on Moodle using the link provided by October 26, 2012. A list of approved testing centers and proctors is given on the Proctor Approval form.

**Completed Proctor Approval Form Deadline October 26, 2012**

Once a proctor has been approved by the professor, the student who plans to take the final exam off-campus must schedule the chapter exam with the proctor at least three weeks prior to the test date. A Test Administration Procedure form will be sent by the instructor to the approved testing center or proctor before the scheduled exam which must be completed by the test administrator and returned to the instructor before the day of the test. Therefore, it is vital for students who plan to take their exam off-campus, complete and upload the Proctor Approval form.

Module Folders

Module folders are a group of files and/or links that are posted on Moodle containing all significant information pertaining to sections being covered during a fixed period of time. The Module folders will include learning objectives, learning activities, lecture notes, assignments, discussion forums and all pertinent information pertaining to weekly activities required to complete the assessments corresponding to the sections that will be covered during a particular time period. The Module folders will be posted weekly according to the dates listed in the Course Outline, the last page of this syllabus, and on the Course Calendar located on the Header Block of the Course Homepage. It is important that students read all documents contained in the Module folders since they contain all instructions on how to meet the requirements each week.

Instruction Sheets

An Instruction Sheet will be posted in each Module folder which will include the learning objectives, and instructions on how to achieve those objectives. Each Instruction Sheet will contain the reading assignments along with the exercise assignment and discussion forum information including due dates.
Exercise Assignments

Exercises will be assigned from the textbook for each section covered. Students are required to complete all exercises. The exercises are used to assess the students’ understanding of the concepts. The students will have one to two weeks to complete each assignment depending on the length and/or complexity of the material. The final grade for the exercise assignments will be based on the average of all exercise assignments and will be worth 50% of the semester grade. The students will be required to upload all completed assignments in the corresponding Module folder on Moodle. Instructions on how to access and submit assignments will be provided by the instructor on the Moodle Homepage.

Since this is the first time this course is being offered, the topics are tentative, so there is a good chance the Course Outline on the last page of this syllabus will be modified. You will be notified when changes are made via email and on the Announcements section of Moodle.

Discussion Forums

Discussion Forums will be posted on Moodle in the Module folders. Each discussion forum will be worth 10 points. These assignments are to help facilitate discussions with your fellow classmates as well as receive comments from the instructor. The first forum will be for the purpose of introducing yourself to the class. The subsequent forums will correspond to the learning objectives and readings and will be located in the Module folders. Due dates will be given when the forum is posted. You will be required to post your answer to the question and to reply to at least one of your classmate’s post. The final grade for discussion forums will be based on the average of all forum grades. The discussion activities will be worth 5% of the semester grade. The criteria for grading the forums is on the Course Homepage on Moodle.

Netiquette
When posting on forums and writing emails, the students must always follow the rules of netiquette. These rules can be found at http://www.albion.com/netiquette/corerules.html.

Late Submission of Exercise Assignments and Discussion Forums

Without prior permission from the instructor, students who submit the exercise assignments and forums late will be penalized. If a student needs more time on a particular assignment he or she must contact the instructor in advance to get permission to avoid a penalty. Without instructor permission, if a student submits an exercise assignment or posts on a forum after the deadline, but before the instructor grades the assignments, the student will be penalized 20%. If a student submits an exercise assignment after the instructor has already graded the assignment, the student will be penalized 50%. If the student has not posted on the Discussion Forum by the time the instructor grades it, the student will receive a zero. I am aware that many of you have jobs and families, and unexpected things may occur during the semester. Therefore, it is very important to stay in contact with the instructor if you will be late on any assignment. Do not wait until after the assignment is due to ask for an extension.

Final Exam

There will be a final exam worth 45% of the semester grade. Students who live out-of-state, or students who do not live within a reasonable driving distance to Nicholls’ campus, may request an alternative location (an approved testing center) to take the exam. Arrangements need to be made by the student in advance. Please see the “Proctor Requirements” section of the syllabus.

**On-campus Final Exam—Tuesday, December 11, 2012 at 10:00 AM**

Semester Grade

The semester grade will be calculated on a ten point grading scale 90-100 A, 80-89 B, 70-79 C, 60-69 D, below 60 F.

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exercise Assignments</td>
<td>50%</td>
</tr>
<tr>
<td>Discussion Forums</td>
<td>5%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>45%</td>
</tr>
</tbody>
</table>

Policies and Procedures

Attendance Policy

Participation in activities is required where an electronic record which clearly indicates time and date activity was submitted. For financial aid purposes, student must complete at least one activity, which is equivalent to having attended at least one class.

Behavioral Policy

Students must at no time be disrespectful toward the Professor. Students must always respect the rights of classmates. Students must behave in a professional manner at all times. Failure to act in an appropriate manner will not be tolerated.
Academic Dishonesty Policy
Cheating will not be tolerated. Sanctions for academic cheating, plagiarism, and forgery of academic documents including signing another's name (Sec 1.9) are those outlined in the Code of Student Conduct handbook. You may access a copy of the handbook by clicking on the following link: http://www.nicholls.edu/documents/student_life/code_of_conduct.pdf.

Academic Grievances
The proper procedure for filing grade appeals or grievances related to academic matters is listed in Section 5 of the Code of Student Conduct handbook.

Continued Learning Following an Extreme Emergency:
In order to make continued learning possible following an extreme emergency;

Students are responsible for:
- reading regular emergency notifications on the NSU website;
- knowing how to use and access Moodle (or university designated electronic delivery system);
- being familiar with emergency guidelines;
- evacuating textbooks and other course materials;
- knowing their Moodle (or designated system) student login and password;
- contacting faculty regarding their intentions for completing the course.

Faculty are responsible for:
- their development in the use of the Moodle (or designated) software;
- having a plan for continuing their courses using only Moodle and email;
- continuing their course in whatever way suits the completion of the course best, and being creative in the continuation of these courses;
- making adjustments or compensations to a student’s progress in special programs with labs, clinical sequences or the like, only in the immediate semester following the emergency.

Americans with Disabilities Act: Students with a documented disability are entitled to classroom accommodations under the ADA. To receive accommodations, contact the Office of Disability Services at (985) 448-4430 or 158-A Shaver Gym. Additional information can be obtained at the following website http://www.nicholls.edu/disability/.

**The last day to drop this course with a “W” is Wednesday, November 7, 2012**
<table>
<thead>
<tr>
<th>MODULE FOLDERS</th>
<th>SECTIONS</th>
<th>Date Posted</th>
<th>Due by 11:59 PM on the given date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 1</td>
<td>(Chapter 1 is just an Overview) 1.1 Secure Communications 1.2 Cryptographic</td>
<td>8/22/12</td>
<td>No Assignment</td>
</tr>
<tr>
<td></td>
<td>2.1 Shift Ciphers 2.2 Affine Ciphers 2.3 The Vigenère Cipher</td>
<td>8/22/12</td>
<td>9/12/12</td>
</tr>
<tr>
<td>Holiday</td>
<td>Labor Day 9/3/12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module 2</td>
<td>2.4 Substitution Ciphers 2.5 Sherlock Holmes 2.6 The Playfair and ADFGX Ciphers 2.7 Block Ciphers</td>
<td>9/7/12</td>
<td>9/19/12</td>
</tr>
<tr>
<td>Module 3</td>
<td>2.8 Binary Numbers and ASCII 2.9 One-Time Pads 2.10 Pseudo-random Bit Generation 2.11 LFSR Sequence 2.13 Enigma</td>
<td>9/14/12</td>
<td>9/26/12</td>
</tr>
<tr>
<td>Module 4</td>
<td>2.10 Pseudo-random Bit Generation 2.11 LFSR Sequence 2.13 Enigma</td>
<td>9/21/12</td>
<td>10/3/12</td>
</tr>
<tr>
<td>Module 5</td>
<td>4.1 Introduction 4.2 A simplified DES-Type Algorithm 4.4 DES 4.5 Modes of Operation</td>
<td>9/28/12</td>
<td>10/10/12</td>
</tr>
<tr>
<td>Module 6</td>
<td>4.6 Breaking DES 4.7 Meet-in-the-Middle Attacks 4.8 Password Security</td>
<td>10/5/12</td>
<td>10/17/12</td>
</tr>
<tr>
<td>Module 7</td>
<td>5.1 The Basic Algorithm 5.2 The Layers 5.3 Decryption</td>
<td>10/12/12</td>
<td>10/24/12</td>
</tr>
<tr>
<td>Module 8</td>
<td>6.1 The RSA Algorithm 6.2 Attacks on RSA</td>
<td>10/19/12</td>
<td>10/31/12</td>
</tr>
<tr>
<td>Module 9</td>
<td>6.3 Primality Testing 6.4 Factoring 6.5 The RSA Challenge</td>
<td>10/26/12</td>
<td>11/7/12</td>
</tr>
<tr>
<td>Module 10</td>
<td>6.6 An Application to Treaty Verification 6.7 The Public Key Concept</td>
<td>11/2/12</td>
<td>11/14/12</td>
</tr>
<tr>
<td>Module 11</td>
<td>To be announced</td>
<td>11/9/12</td>
<td>11/30/12</td>
</tr>
<tr>
<td>Holiday</td>
<td>Thanksgiving 11/19/12 – 11/23/12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FINAL EXAM</td>
<td>On-campus Final Exam—Tuesday, December 11, 2012 at 10:00 AM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**The last day to drop this course with a “W” is Wednesday, November 7, 2012**