Applied Cryptography

Course Description
This course includes an introduction to cryptographic algorithms and protocols for encrypting information securely, techniques for analyzing vulnerabilities of protocols, approaches to digital signatures and information digests, and implementation approaches for the most significant cryptographic methodologies.

Learning Objectives
1. Identify and prioritize cryptographic issues
2. Analyze and describe specific cryptographic techniques
3. Identify, analyze, and counteract threats to cryptographic protocols
4. Define and analyze actual cases of cryptographic protocol failures
5. Understand and analyze digital cash protocols and mechanisms
6. Compare and contrast electronic voting protocols
7. Describe and analyze digital signature methodologies
8. Test cryptographic algorithms and protocols using open source tools

Major Course Requirements

Problem Sets. Problem sets will be assigned from the text as well as from other sources. Unix command based tools such as OpenSSL will be used for some of the assignments. For problem sets, you are allowed to discuss with other students in general terms, but you must not copy and submit someone's work as your own for credit. Some programming problems may be assigned; however, it depends on the background of the students in the class.

Paper. This course requires that you write a technical paper related to cryptography. List of topics and relevant resources will be made available to the class later. The paper is due at the end of the semester. There will be a presentation session for all papers at the end of the semester.

Examinations. Two exams will be given. The first exam will be given on Wednesday, October 13, 2014. The second exam will be given on December 1, 2014.

Semester grades will be based on the following weights:

<table>
<thead>
<tr>
<th>Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam 1</td>
<td>30%</td>
</tr>
<tr>
<td>Assignments</td>
<td>25%</td>
</tr>
<tr>
<td>Paper</td>
<td>15%</td>
</tr>
<tr>
<td>Exam 2</td>
<td>30%</td>
</tr>
</tbody>
</table>
Required or Recommended Readings


**Website:** TBD

**List of Supplies:** None

Various related resources including the ones available on the Internet will be used to cover advanced and contemporary topics on algorithms and protocols (such as AES, elliptic curve cryptography).

Course Policies

**Attendance/Tardiness**

You must attend all classes. You are responsible for any materials covered or handed out or announcements made for the tests, quizzes, and homework assignments in your absence. Records of your attendance will be maintained and reported to the university. Students found missing classes without the instructor's permission will be automatically withdrawn from the course. Students are responsible for all materials covered in class and assigned. Should a student be absent from class, it is his/her responsibility to get the notes, etc. for that missed class. More important, should there be assignments, it is the student’s responsibility to obtain such assignments. No excuse will be accepted for assignments not turned in because the student was absent when it was due.

**Late Work and Make-up Exams**

All the assignments are due at the beginning of the class on the due date. If the student is absent on the assignment due date, it is the student's responsibility to make sure that the assignment is submitted on the designated date. An assignment that is turned in after the class on the due date is considered one day late. There is a penalty for late submissions. Late assignments will be counted 20% off for each day after the due time. No credit will be given if an assignment is submitted after 5 days. If you have not completed your assignment by the due date, you should submit the work you have done for partial credit. No work will be accepted once the graded work has been returned or the solution has been disclosed to the class, except for unusual circumstances.

Exams must be taken on the hour they are scheduled. In the event, if you cannot attend the class to take the exam due to some emergency or some unavoidable
situation (such as serious illness, death in the family, participation in university sports, religious observations, and so on) you must notify me as soon as possible before the exam and also you must validate your absence by providing me a document (e.g., with a letter from your doctor).

**Extra Credit**

None

**Cell Phone/Electronic Device Usage**

Set your cell phone/electronic device in silent mode when you are in class.

**Academic Integrity/Plagiarism**

University students are expected to conduct themselves in accordance with the highest standards of academic honesty. Academic misconduct for which a student is subject to penalty includes all forms of cheating, such as illicit possession of examinations or examination materials, falsification, forgery, complicity or plagiarism. (Plagiarism is the presentation of the work of another as one’s own work.) In this class, academic misconduct or complicity in an act of academic misconduct on an assignment or test will result in a score of 0 (zero) for the work or dismissal from the course and the Dean of Students office will be notified. No copying from another student's work, of any class, is allowed. It is the student's duty to allow no one to copy his or her work. Anyone found cheating in the exams will receive an automatic F for the course.

**Dropping a Class**

I hope that you never find it necessary to drop this or any other class. However, events can sometimes occur that make dropping a course necessary or wise. Please consult with me before you decide to drop to be sure it is the best thing to do. Should dropping the course be the best course of action, you must initiate the process to drop the course by going to the Student Services Center and filling out a course drop form. Just stopping attendance and participation WILL NOT automatically result in your being dropped from the class. November 7, 2014 is the last day to drop a class with an automatic grade of “W” this term.

**Preferred methods of scholarly citations**

All referenced material used in a paper or project report must be properly acknowledged and cited. Use APA style for all scholarly citations.

**Classroom/professional behavior**

Texas A&M University-Corpus Christi, as an academic community, requires that each individual respect the needs of others to study and learn in a peaceful atmosphere. Under Article III of the Student Code of Conduct, classroom behavior that interferes with either (a) the instructor’s ability to conduct the class
or (b) the ability of other students to profit from the instructional program may be considered a breach of the peace and is subject to disciplinary sanction outlined in article VII of the Student Code of Conduct. Students engaging in unacceptable behavior may be instructed to leave the classroom. This prohibition applies to all instructional forums, including classrooms, electronic classrooms, labs, discussion groups, field trips, etc.

**Statement of Civility**

Texas A&M University-Corpus Christi has a diverse student population that represents the population of the state. Our goal is to provide you with a high quality educational experience that is free from repression. You are responsible for following the rules of the University, city, state and federal government. We expect that you will behave in a manner that is dignified, respectful and courteous to all people, regardless of sex, ethnic/racial origin, religious background, sexual orientation or disability. Behaviors that infringe on the rights of another individual will not be tolerated.

**Grade Appeals**

As stated in University Procedure 13.02.99.C2.01, Student Grade Appeal Procedures, a student who believes that he or she has not been held to appropriate academic standards as outlined in the class syllabus, equitable evaluation procedures, or appropriate grading, may appeal the final grade given in the course. The burden of proof is upon the student to demonstrate the appropriateness of the appeal. A student with a complaint about a grade is encouraged to first discuss the matter with the instructor. For complete details, including the responsibilities of the parties involved in the process and the number of days allowed for completing the steps in the process, see University Procedure 13.02.99.C2.01, Student Grade Appeal Procedures. These documents are accessible through the University Rules website at http://www.tamucc.edu/provost/university_rules/index.html, and the College of Science and Engineering Grade Appeals webpage (http://sci.tamucc.edu/students/GradeAppeal.html). For assistance and/or guidance in the grade appeal process, students may contact the chair or director of the appropriate department or school, the Office of the College of Science and Engineering Dean, or the Office of the Provost.

**Disabilities Accommodations**

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation, please call or visit Disability Services at (361) 825-5816 in Corpus Christi Hall 116.

If you are a returning veteran and are experiencing cognitive and/or physical access issues in the classroom or on campus, please contact the Disability Services office for
assistance at (361) 825-5816.

**Statement of Academic Continuity**
In the event of an unforeseen adverse event, such as a major hurricane and classes could not be held on the campus of Texas A&M University–Corpus Christi; this course would continue through the use of Blackboard and/or email. In addition, the syllabus and class activities may be modified to allow continuation of the course. Ideally, University facilities (i.e., emails, web sites, and Blackboard) will be operational within two days of the closing of the physical campus. However, students need to make certain that the course instructor has a primary and a secondary means of contacting each student.

**Content Topics**

- Cryptographic protocol fundamentals
- Communications using symmetric cryptography
- Communications using public-key cryptography
- Key exchange, timestamping, digital signatures, bit commitment,
- Zero-knowledge proofs, blind signatures, oblivious transfer, simultaneous contract signing
- Secure elections and digital cash
- Key length and key management
- Cryptographic algorithm types and modes
- Mathematical background for cryptographic algorithms
- Block ciphers: DES and AES
- Stream ciphers and pseudo-random-sequence generators
- One-way hash functions: MD5, SHA
- Public-key algorithms: RSA, elliptic curve cryptography, identity based encryption
- Identification schemes
- Key-exchange algorithms
- Special algorithms for protocols
- OpenSSL and other open source tools