Applied Cryptography COSC 5377  
Department of Computing Sciences  
Fall 2017

A. COURSE INFORMATION
   Course number/section:  COSC 5377  
   Class meeting time:  TR 3:30 – 4:45 p.m.  
   Class location:  IH-164  
   Course Website:  TBA

B. INSTRUCTOR INFORMATION
   Instructor:  Dr. Dulal Kar  
   Office location:  CI-321  
   Office hours:  11:30 a.m. – 12:30 p.m. (MW) and 2:00 p.m. – 3:30 p.m. (TR)  
   Telephone:  361-825-5878  
   e-mail:  dulal.kar@tamucc.edu  
   Appointments:  By e-mail

C. COURSE DESCRIPTION
   Catalog 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.

   Extended Course Description
   None

D. PREREQUISITES AND COREQUISITES
   Prerequisites
   None.
   Corequisites
   None.

E. REQUIRED TEXTBOOK(S), READINGS AND SUPPLIES
   Required Textbook(s)

   Optional Textbook(s) or Other References
   None. However, 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, and identity based encryption).

**Supplies**

None.

**F. STUDENT LEARNING OUTCOMES AND ASSESSMENT**

Assessment is a process used by instructors to help improve learning. Assessment is essential for effective learning because it provides feedback to both students and instructors. A critical step in this process is making clear the course’s student learning outcomes that describe what students are expected to learn to be successful in the course. The student learning outcomes for this course are listed below. By collecting data and sharing it with students on how well they are accomplishing these learning outcomes students can more efficiently and effectively focus their learning efforts. This information can also help instructors identify challenging areas for students and adjust their teaching approach to facilitate learning.

By the end of this course, students should be able to:

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

**G. INSTRUCTIONAL METHODS AND ACTIVITIES**

Instructions will be delivered through in-class lectures and presentations using slides. Students will be required to present their papers or projects in the class.

**H. MAJOR COURSE REQUIREMENTS AND GRADING**

**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 on the final exam day as scheduled by the university.

Exams. Two exams will be given. The first exam will be given on October 12, 2017. The second exam will be given on December 4, 2017.

<table>
<thead>
<tr>
<th>ACTIVITY</th>
<th>% of FINAL GRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exams</td>
<td>60</td>
</tr>
<tr>
<td>Homework and Quizzes</td>
<td>25</td>
</tr>
<tr>
<td>Presentation</td>
<td>5</td>
</tr>
<tr>
<td>Paper</td>
<td>10</td>
</tr>
</tbody>
</table>

I. COURSE CONTENT/SCHEDULE

<table>
<thead>
<tr>
<th>DATE (BY DAY OR WEEK)</th>
<th>TOPIC</th>
<th>CHAPTER(S)</th>
<th>ASSIGNMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cryptographic protocol fundamentals</td>
<td>Chapter 1</td>
<td>TBD</td>
</tr>
<tr>
<td>2</td>
<td>Communications using symmetric and public key cryptography</td>
<td>Chapter 2</td>
<td>TBD</td>
</tr>
<tr>
<td>3</td>
<td>Key exchange, timestamping, digital signatures, and bit commitment protocols</td>
<td>Chapters 3 and 4</td>
<td>TBD</td>
</tr>
<tr>
<td>4</td>
<td>Block ciphers: DES and AES</td>
<td>Chapter 12 and online resource</td>
<td>TBD</td>
</tr>
<tr>
<td>5</td>
<td>Stream ciphers Key length and key management Cryptographic algorithm types and modes</td>
<td>Chapters 7-9</td>
<td>TBD</td>
</tr>
<tr>
<td>6</td>
<td>Zero-knowledge proofs, blind signatures, oblivious transfer, simultaneous contract signing</td>
<td>Chapter 6</td>
<td>TBD</td>
</tr>
<tr>
<td>7</td>
<td>Exam 1, October 12, 2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Mathematical background for cryptographic algorithms</td>
<td>Chapter 11</td>
<td>TBD</td>
</tr>
<tr>
<td>Week</td>
<td>Topic</td>
<td>Chapter</td>
<td>Due Date</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>9</td>
<td>Secure elections and digital cash</td>
<td>Chapter 6</td>
<td>TBD</td>
</tr>
<tr>
<td>10</td>
<td>One-way hash functions: MD5, SHA</td>
<td>Chapter 18</td>
<td>TBD</td>
</tr>
<tr>
<td>11</td>
<td>Public-key algorithms: RSA algorithm and El-Gamal algorithm</td>
<td>Chapter 19</td>
<td>TBD</td>
</tr>
<tr>
<td>12</td>
<td>Digital signature algorithms, Key-exchange algorithms, Diffie-Hellman and Hughes protocols</td>
<td>Chapter 20 and Chapter 22</td>
<td>TBD</td>
</tr>
<tr>
<td>13</td>
<td>Elliptic curve cryptography, identity based encryption</td>
<td>Online resource</td>
<td>TBD</td>
</tr>
<tr>
<td>14</td>
<td>Special algorithms for protocols OpenSSL and other open source tools</td>
<td>Online resource</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td><strong>Exam 2: December 4, 2017</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><strong>Final Exam: Paper Presentations (December 12, 2017 from 1:45 p.m. – 4:15 p.m.)</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Changes in this course schedule may be necessary and will be announced to the class by the Instructor. The assignments and exams shown are directly related to the Student Learning Outcomes described in Section F.

### J. COURSE POLICIES

**Course Syllabus:** We will meet for lecture on Tuesdays and Thursdays, when new material will be presented. We will follow the text generally, but non-text material may also be included in the lectures. The assignments and exams will be given during the class hours. You are responsible for all the material presented during the lecture.

**Exams:** Exams will cover all lecture and reading material discussed in the class. Exams must be taken on the hour they are scheduled.

**Missed Exams:** 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). Once your cause is validated a make-
up exam will be given.

**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:** 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.

**Academic Honesty Policy:** You are expected to avoid all forms of academic dishonesty as defined in Catalog. In addition, students are expected to behave in an ethical manner in all class activities. If you feel uncertain about a particular activity, please speak to me BEFORE problems arise. Ethical behavior is a requirement for passing this course. All work submitted for grading must be the student's own work. Plagiarism 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 and/or copying, in the exams or assignments, in the instructor's opinion, will receive an automatic F for the course.

**Collaboration:** If two or more people collaborate on an assignment assigned it should be notified on the assignment and each student should submit his or her solutions for grading. The grade obtained on such an assignment is the total points obtained for the assignment divided by the square of the number of people who collaborated on the assignment (e.g., if 3 people collaborate on an assignment and the grade for that assignment is 90 out of 100, then each student receives a grade of 90/3² = 10). If you do not notify me of such collaboration it will be treated as copied and action will be taken as discussed under the academic honesty policy.

**Extra Credit**
None.
Cell Phone Use
Set your cell phone/electronic device in silent mode when you are in class.

Laptop Use
You can only use your laptop to view course documents or slides.

Food in Class
Not allowed.

Participation
You are encouraged to ask questions related to course topics that can help you and others attending the class.

K. COLLEGE AND UNIVERSITY POLICIES

• Academic Integrity (University)
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 failing grade.

• 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.

- **Deadline for Dropping a Course with a Grade of W (University)**
  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 your academic advisor, the Financial Aid Office, and me, before you decide to drop this course.* 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. Please consult the Academic Calendar ([http://www.tamucc.edu/academics/calendar/](http://www.tamucc.edu/academics/calendar/)) for the last day to drop a course.

- **Grade Appeals (College of Science and Engineering)**
  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](http://www.tamucc.edu/provost/university_rules/index.html), and the College of Science and Engineering Grade Appeals webpage at [http://sci.tamucc.edu/students/GradeAppeal.html](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.

- **Disability Services**
  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 (361) 825-5816 or visit Disability Services 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.
http://disabilityservices.tamucc.edu/

- **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.

A. **OTHER INFORMATION**
- **Academic Advising**
  The College of Science & Engineering requires that students meet with an Academic Advisor as soon as they are ready to declare a major. The Academic Advisor will set up a degree plan, which must be signed by the student, a faculty mentor, and the department chair. Meetings are by appointment only; advisors do not take walk-ins. Please call or stop by the Advising Center to check availability and schedule an appointment. The College’s Academic Advising Center is located in Center for Instruction 350 or can be reached at (361) 825-3928.

**GENERAL DISCLAIMER**
I reserve the right to modify the information, schedule, assignments, deadlines, and course policies in this syllabus if and when necessary. I will announce such changes in a timely manner during regularly scheduled lecture periods.