Course Description

From the 2011-2012 Course Catalog - TCOM 556: Title: Cryptography and Network Security  
Prerequisites: TCOM 500 and 548. Description: Broad overview of cryptographic algorithms and mechanisms, and application in today's communication networks. Discusses modern cryptographic techniques such as public key cryptography, digital signatures, secret sharing, key management, key escrow, public key certificates, and public key infrastructure. Covers cryptography on Internet including secure electronic mail, secure WWW, and electronic commerce. Compares, analyzes software implementations of cryptographic algorithms.

NOTE: Students will provided appropriate documentation to the instructor to ensure that all prerequisites have been met prior to taking this course.

Note: This course extensively uses Microsoft Excel or LibreOffice Calc spreadsheets for projects and exercises.

Note: This course does not require nor expect a background in Computer Science (CS), Electrical and Computer Engineering (ECE), Computer Networking, or Information Security.

Course Objectives

To provide a broad-ranging introduction to the complexity of security and privacy issues within telecommunications. The intent of this course is for students to understand and digest the complex and often subtle telecommunications security, privacy and cryptographic issues and philosophy before engineering design mistakes are made. This means that if you are looking for "hands on" or "how to" then this is probably the wrong class to attend. In general, mathematics will not be required for this course, though students may be expected to apply design approaches and understand tools that involve numerical manipulation. The emphasis for these courses will be placed on practical tools and examples using rational rather than on mathematical rigor.

This course may be a challenge for some, easy for others. This course are being taught with premise that the academia setting is correct and appropriate place to explore and contribute to the philosophy of cryptography and network security. Therefore, if you are unwilling to question the fundamental nature of security and cryptography then you will not do as well as you might think. On the other hand, if you are unable to work with and contribute in a positive manner to the class then you may also not do so well. Keep these things in mind, take notes and keep up with the discussions and you should do well.

At the conclusion of this course, students should have a basic ability to:

• Understand, discuss and appreciate the fundamental concepts of network security and cryptography and the principle trade-offs involved.
• Discriminate between conditional approaches to information security concepts.
• Be able to evaluate complex technical proposals concerning security auditing, intrusion detection, etc., and lead oral and written efforts for the evaluation of damage assessment and security control arrangement teams.
• Communicate effectively in leading computer scientists, engineers and decision experts responsible for the technical elements involved in designing, developing, and operating advanced information security systems in a rational way.

Email

Email is the recommended and preferred mode of communications with the instructor. Answers to technical questions may be redistributed to other students via E-mail or on blackboard. You are expected to have and use your GMU E-mail address for this course. Check the course blackboard site regularly for updates and announcements as applicable.

NOTE: email is not a real-time communications facility, therefore, the instructor will not be able to respond to student email messages instantly. The earliest that the instructor may be able to respond to email is no less than 24 hours.
Attendance

Please arrive on time. Not taken for credit at lecture, but you are responsible for all material presented in class/lab whether or not it is in the published notes. Therefore, consistent and weekly attendance is strongly recommended in order to achieve the highest course grade. If you are late for class, please enter the class quietly and sit by the entrance to minimize the disturbance to the rest of the class. An attendance sign-up sheet will be distributed sometime during the class. Please sign only your name. I expect to start at 7:20pm sharp. Please participate in class! Ask questions if there is something you don't understand.

Lectures

Recording of lectures with any type of electronic or electro-mechanical recording device is not permitted.

Some class sessions will be part lecture and part exercises (second half of session) while others are all lecture based.

Lecture sessions may include current developments (i.e., events) in the area of computer and network security and privacy.

Caution: Not every slide will be covered during a lecture session.

Lecture Slides

The lecture slides for the Cryptography and Network Security book are available from the course textbook instructor resource page for Crypto-05e. Note: Instructor slides shown in class contain may contain corrections to those provided by the authors. Caution: Not every slide will be covered during a particular lecture session.

Some lecture material will be from external sources (not contained in the class slides).

Distance Learning

Distance learning section is offered synchronously via the web using Blackboard Collaborate. Collaborate student instructions and guidelines for quizzes and exams are posted on Backboard. Distance learning tools may be used during the semester to compensate when the Instructor is off-campus. http://distance.gmu.edu/. If students have any problems in connecting to a collaborate session, students are to contact the ITU support center at 703-993-8870 during business hours or at http://itusupport.gmu.edu; or the CLUB-Collaborative Computer Lab at 703-993-3141 or by e-mail at club@gmu.edu; CLUB URL: http://doit.gmu.edu/staffSection.asp?page=club.

Homework Assignments

Homework assignments and projects are posted on blackboard and/or given in class. The objective of the homework assignments is to keep students knowledgeable of the material covered in the course. Show intermediate work as appropriate when submitting homework assignment answers.

All homework assignments and projects are due BEFORE the start of class session (i.e., homework review/lecture) on the due date. If and only if you are not able to submit your homework assignment in class, you may submit via email on or before the due date/time to the TA with a courtesy copy (cc:) to the instructor. The student is responsible for ensuring that email submitted homework is received before the due date/time. Thus, the student needs to account for possible delivery delays of email systems. Unless arrangements are worked out in advance, missed assignments cannot be made up. When submitting homework electronically, ensure that files are in .PDF format.

In recognition of the fact that many students have occasional but unavoidable work and family commitments that preclude attendance at every class, the lowest single homework assignments will be dropped prior to final grade computations. In view of this policy, late homework is not accepted. Please don't ask for an exception. No project scores are dropped.

All Homework assignments are graded for correctness.

Homework assignments should be neatly typed. Readable handwritten assignments are acceptable.

The instructor may discard unclaimed graded assignments after two weeks have elapsed past the original due date. All unclaimed assignments will be discarded after the final exam. The solutions to the previous week's homework assignment will be discussed at the beginning of class.
Class Demonstrations & Exercises

Throughout the semester in-classroom demonstrations & exercises of various cryptographic tools may be shown or discussed. There will be questions on the exams and quizzes about these demonstrations & exercises.

Text Books

The following textbooks are required:

Title: Secrets and Lies: Digital Security in a Networked World (paperback)
First Edition
Author: Bruce Schneier
Publisher: Wiley Publishers
Publisher Web Site
ISBN: 0471453803
© 2004
Reference Designator: TX1
Textbook Resource: Web Page

Title: Cryptography and Network Security
Fifth Edition
Author: William Stallings
Publisher: Prentice-Hall
Publisher Web Site
ISBN: 0-13-6097049
© 2011
Reference Designator: TX2
Textbook Resource Web Page

References:

NOTE: The Internet/ World Wide Web will be utilized to provide additional sources of course reference material.

Be sure to check the textbook web sites on a regular basis for errata sheet updates.

Note: Textbook references (text.chapter.section) are cited for weekly lecture topics while references for problems follow the format of text.chapter.problem number.

Honor Code

You are encouraged to collaborate with other students for general studying.

Exams are closed book, closed notes, and no use of calculators unless otherwise noted. The normal GMU Honor Code applies to all exams, quizzes, and all homework assignments which carry with them an implicit statement that it is the sole work of the author, unless joint work is explicitly authorized. Help may be obtained from the instructor, or other students to understand the description of the problem and any technology, but the solution, must be the student's own work.

Any deviation from these are considered an Honor Code violation, and as a minimum, will result in failure of the submission and as a maximum, failure of the class.

Plagiarism

You must clearly indicate any and all instances when your work includes, is based on, or is derived from the work of others. Just be sure to include explicit in-line citations where applicable. Any violations are sufficient to receive a failing grade. Refer to GMU's Honor System and Code.

Computer Labs

There are several Computer Labs available for general use by IT&E students, which are located on the Fairfax campus. For more information go to the web site at http://ite.gmu.edu/labs.
Exam Policy

Students who arrive more than fifteen (15) minutes late for any exam will not be permitted to take the exam and will automatically receive a grade of zero for that exam. There may be take home exams.

Makeup exams are very rarely given. Requests for a delayed Final Exam due to multiple tests (>2) in one day will ONLY be considered if proper forms are completed and in the instructor's hands on or before the mid-term grading period ends.

(excerpts) From the 2011-2012 University Catalog:

- A student who misses an exam without an excuse may have the course grade lowered.
- Students must not be required to submit examinations before the date of the regularly scheduled examination for a course. Final reexaminations are not permitted.
- Absence from final examinations will not be excused except for sickness on the day of the examination or for other cause approved by the student's academic dean/director.

From the Schedule of Classes:

- Students who have more than one examination scheduled at the same time or more than two examinations scheduled on the same day should consult their academic dean to request rescheduling.

There will be only one makeup final exam for those students who have received authorization from the instructor to take the final exam at the other than the normally scheduled time. This makeup exam will be given the day following the regularly scheduled final exam at the same time or as announced by the instructor.

Since the College of Arts and Sciences does not have a specific procedure, those students in CAS who are eligible to take the final exam at the makeup exam time should follow the School of IT&E procedures and fill out the appropriate forms and return them to the instructor on or before mid-term grading period ends. No requests for any reason will be accepted after that date.

Exam Formats

The time period for exams covers the entire class session, unless otherwise noted.

- All exams are closed book and notes, unless otherwise specified. Exams are both essay and problem solving based.

The final exam will be comprehensive with a selected number of questions from the first part of the course.

- Exams will cover all material discussed through the prior class (including the current reading assignment) and will emphasize material covered during class lectures, labs, reading and homework assignments.

Reading Assignments

Reading assignments are listed in this syllabus and/or given in class. Students are expected to have read the assigned material before the corresponding lecture in which the material will be discussed. Students are responsible for all material assigned. Reference the Homework and Exam Format section.

Students with Disabilities

If you need special assistance, please inform the instructor soon as possible so that appropriate arrangements can be made. Contact GMU’s Office of Disability Services (Disability Resource Center) for additional information. http://ods.gmu.edu/

Computer and IT Security

Grading Policy

Homework = 20%  Short Quizzes=20%  Projects = 25%  Final Exam = 35%

The final course grade is based on an absolute standard of the weighted sum of all grades (NO grades will be dropped [except where noted] nor a curve applied to the grades).

In recognition of the fact that many students have occasional but unavoidable commitments that preclude attendance at every class, the lowest single homework assignment score is dropped. Attendance at all exams are mandatory.

Plus/Minus grades will be used as indicated:
A+: 100-97  A: 96-93  A-: 92-90  B+: 89-85  B: 84-80  B-: 79-76  Cs: 75-60  Fs: <60

Grade information with students is not communicated via email. Make an appointment with the instructor to discuss.

Quizzes

Quizzes will be normally given during the first 15-45 minutes of class. Quizzes may be unannounced. Students who arrive more than fifteen (15) minutes late for any quiz will not be permitted to take the quiz and will automatically receive a grade of zero for that exam.

Quizzes are closed book and notes, unless otherwise specified.

Exams and quizzes are both essay and problem solving based.

The goal of the quizzes is to keep students abreast of the material covered in class.

In recognition of the fact that many students have occasional but unavoidable work and family commitments that preclude attendance at every class, the lowest single quiz grade will be dropped prior to final grade computations. In view of this policy, there are no make-up quizzes. Please don’t ask for an exception.

Cell Phone & Electronic Device Policy

Turn cell phones and personal communication device ringers in silent mode during class sessions.

Phone calls, text messages, instant messages, email, and general web surfing are not permitted during class time.

Computers may only be used to follow the material in class. Violators will have their devices confiscated or asked to leave the room.

Personal Safety and Security

The Mason Alert system provides emergency information of various sorts. Students can sign up for it by visiting the website https://alert.gmu.edu. Students can also be reminded that an emergency poster exists in each classroom explaining what to do in the event of crises and that further information about emergency procedures exists on http://www.gmu.edu/service/cert.

Diversity

George Mason University promotes a living and learning environment for outstanding growth and productivity among its students, faculty and staff. Through its curriculum, programs, policies, procedures, services and resources, Mason strives to maintain a quality environment for work, study and personal growth.

For more information refer to the following URL: http://cte.gmu.edu/Teaching_at_Mason/DiversityStatement.html
University Catalog

The George Mason University 2011-2012 University Catalog can be found here: [http://catalog.gmu.edu](http://catalog.gmu.edu)

University Policies

The purpose of this University Policy web site is to ensure that the University community has ready access to well-articulated and understandable University policies. Policies that are easy to find, read and understand will help the university accomplish its mission, maintain accountability, provide employees and students with clear and concise guidelines, and clarify how the university conducts business.

For more information refer to the following URL: [http://universitypolicy.gmu.edu](http://universitypolicy.gmu.edu)

Calendar of Religious Holidays and Observations

The Calendar covers the following religious groups: Bahá'í Faith, Buddhist, Catholic, Protestant Christian denominations, Hindu, Jewish, Muslim, and Orthodox Christian.

**It is the student's responsibility to speak to the instructor in advance in the event that their religious observances will impact their participation with course activities and assignments.**

For more information refer to the following URL: [http://ulife.gmu.edu/religious_calendar.php](http://ulife.gmu.edu/religious_calendar.php)

Academic Calendar

University academic calendar can be found here: [http://registrar.gmu.edu/calendars/](http://registrar.gmu.edu/calendars/)

Student Responsibilities

Students are expected to attend all classes or view the class via distance learning either live or afterwards. Students are to attend class with the necessary class notes/materials made available on blackboard as they will not be handed out in class nor email. Reading and homework assignments are expected to be completed outside class hours. Students are responsible for any material covered during an absence, even if that material was supplementary and not in the textbook or lecture notes. When a class is canceled, scheduled assignments or exams are re-scheduled for the next time the class meets. Students are required to regularly check Blackboard for updates.

Professionalism

Students are expected to behave in a professional manner in the classroom and to mute their microphones during distance learning attendance. Consequently, student should turn off all cell phones, blackberries, smartphones, and other electronic devices during class. Students are expected to behave courteously and politely towards other students and the instructor. Disciplinary action may be initiated against a student who disrupts the class environment.

Updates

As the semester progresses, course materials and notices about changes to the course are posted on [blackboard](http://blackboard.gmu.edu).

Wishing you a great semester!
## Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Activity</th>
<th>Reading Assignment Due</th>
<th>Homework/Project Assignment Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>12-18 March</td>
<td>SPRING BREAK</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>19 Mar</td>
<td>Introduction/Course Overview (Syllabus Review) Computer &amp; Network Security &amp; Privacy Overview Introduction, Digital Threats, Security Needs</td>
<td>TX1: Chpts 1, 2 &amp; 5 TX2: §1.1 → 1.8</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>26 Mar</td>
<td>Cryptography, Cryptography in Context Classical Encryption Techniques Foundations</td>
<td>TX1: Chpts 6 &amp; 7 TX2: §2.1 → 2.7 Skim Hill Cipher</td>
<td>TX1: - TX2: R1-1 → R1-5, P1.1, 1.4</td>
</tr>
<tr>
<td>3</td>
<td>2 Apr</td>
<td>Block Ciphers and DES</td>
<td>TX2: §3.1 → 3.4, §3.6 → 3.7 Appendices C &amp; 4A</td>
<td>TX2: R2-1 → R2-5, R2-7; P2.1, P2.2, P2.3, P2.10, P2.11, P2.17; Project #1</td>
</tr>
<tr>
<td>4</td>
<td>9 Apr</td>
<td>Block Ciphers (continued) - AES</td>
<td>TX2: §5.2 → 5.5, 5.7 Appendices 5B and E</td>
<td>TX2: R3-1, R3-2, R3-5, R3-7; P3.8</td>
</tr>
<tr>
<td>5</td>
<td>16 Apr</td>
<td>Certificates and Credentials Public Key Cryptography &amp; RSA, Key Management, Digital Signatures and Authentication Protocols</td>
<td>TX1: Chpt 15, 19 TX2: §9.1 → 9.4, §10.1, 10.2, 10.5, 10.6, §13.1 - 13.5</td>
<td>TX1: - TX2: R5-5; P5.6 Project #2</td>
</tr>
<tr>
<td>-</td>
<td>21 Apr</td>
<td>Visit &amp; Tour – National Cryptologic Museum Ft. Meade, MD</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>30 Apr</td>
<td>Firewalls</td>
<td>TX2: §22.1 → 22.4</td>
<td>TX2: R18-1, R18-3, R19-1, R19-2, R19-4 Project #3</td>
</tr>
<tr>
<td>-</td>
<td>7 May</td>
<td>READING DAY – NO CLASSES</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>14 May</td>
<td>Final Exam (7:30 pm → 10:15 pm)</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Note:** Textbook references (text.chapter.section) are cited for weekly lecture topics while references for problems/exercise follow the format of text:chapter.exercise number

**NOTE:** Review questions are indicated explicitly as prefixed above with R-Question; Problems questions are indicated explicitly as prefixed above with P.

**Textbook References:**


**NOTE:** Schedule is subject to change; check blackboard for most current schedule.

**NOTE:** **Late Homework and Projects are Not Accepted**