Syllabus  revised 9/9/2021

University Policies

The University Catalog is the central resource for university policies affecting student, faculty, and staff conduct in university affairs. Unless explicitly noted, any conflict between the policies in the University Catalog and the content of this document is unintentional. Please notify the author to resolve any such conflicts.

Please note that the Academic Year runs from the Fall semester of one calendar year through the Spring and Summer semesters of the following calendar year. Please be sure to select the correct archived Catalog if appropriate.

Scheduled Sections

<table>
<thead>
<tr>
<th>Section</th>
<th>Instructor</th>
<th>Campus</th>
<th>Day</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL2</td>
<td>Prof. Lyons</td>
<td>Online</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Access to Blackboard for each section will be made available no later than the day of the first class for that section.
Course Description

From the University Catalog:

AIT 682: Network and Systems Security. 3 credits.

Introduces the principles and practices of cryptography, network security, and secure software by covering security policies, models, and mechanisms for secrecy, integrity, and availability; basic cryptography and its applications; secret key cryptography; hash functions; basic number theory and public key cryptography; trusted intermediaries, and network security (firewalls, IDS, IPsec, and SSL) etc. Offered by Info Sciences & Technology. May not be repeated for credit.

Recommended Prerequisite: AIT 660.

Registration Restrictions:

Enrollment limited to students with a class of Advanced to Candidacy, Graduate, Junior Plus or Non-Degree.

Enrollment is limited to Graduate or Non-Degree level students.

Students in a Non-Degree Undergraduate degree may not enroll.

Enrollment limited to students in the Volgenau School of Engineering college.

Schedule Type: Lecture

Grading:
This course is graded on the Graduate Regular scale.

Prerequisites

AIT 660 is the recommended prerequisite course. Students are advised to take that course prior to (not concurrent with) this course in order to develop competency in the fundamentals of cybersecurity, unless they have already completed equivalent coursework.

Rationale

This course covers the foundations of network security and systems security.
Objectives

On successful completion of this course, students will understand:

- security policies and security models;
- security mechanisms for confidentiality, integrity, and availability;
- basic cryptography and its applications;
- secret key cryptography and public key cryptography;
- the functions and usages of network security tools.

Faculty and Staff

Course Coordinator:

Dr. Sun

Instructors:

See Scheduled Sections above.

See links to faculty home pages for information on office hours, contact preferences, etc.

Teaching Assistants:

To be assigned – see Blackboard

Administrative support:

Department of Information Sciences and Technology
Fairfax campus
5400 Nguyen Engineering Building
Email: msait@gmu.edu
Phone: 703-993-3565
References

Textbooks

There is one required textbook for this course:

Network Security: Private Communication in a Public World
2nd edition
Charlie Kaufman, Radia Perlman, Mike Speciner
© 2002; Pearson

Grading

Grades will be awarded in accordance with the Mason Grading System for graduate students. See AP.3.1 Graduate Grading for more information.

The grading scale for this course is:

<table>
<thead>
<tr>
<th>Raw Score</th>
<th>Percentage</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>97 - 100%</td>
<td>100%</td>
<td>A+</td>
</tr>
<tr>
<td>93 - 96%</td>
<td>A</td>
<td>Passing</td>
</tr>
<tr>
<td>90 - 92%</td>
<td>A-</td>
<td>Passing</td>
</tr>
<tr>
<td>87 - 89%</td>
<td>B+</td>
<td>Passing</td>
</tr>
<tr>
<td>83 - 86%</td>
<td>B</td>
<td>Passing</td>
</tr>
<tr>
<td>80 - 82%</td>
<td>B-</td>
<td>Passing</td>
</tr>
<tr>
<td>70 - 79%</td>
<td>C</td>
<td>Passing but unsatisfactory</td>
</tr>
<tr>
<td>0 - 69%</td>
<td>F</td>
<td>Failing</td>
</tr>
</tbody>
</table>

Raw scores may be adjusted by the Instructor to calculate final grades.
Final grades will be determined based on the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework</td>
<td>20%</td>
</tr>
<tr>
<td>Term project</td>
<td>30%</td>
</tr>
<tr>
<td>Mid-term exam</td>
<td>20%</td>
</tr>
<tr>
<td>Final exam</td>
<td>30%</td>
</tr>
</tbody>
</table>

These components are outlined in the following sections.

**Homework**

Homework will be assigned throughout the semester. Each assignment will count towards the final grade - there are no "optional" assignments. Each homework assignment is to be prepared and submitted by the individual student as specified by the Instructor.

**Term project**

Each student will submit a proposal for an individual term project. When the proposal has been graded (and revised as necessary), the student will research relevant topics and submit a report. Further details will be discussed in lectures.

**Mid-term exam**

The mid-term exam will be held online during the eighth scheduled class session. Students will receive feedback on the grading of their exams.

**Final exam**

The final exam will be held online during the final exam period. Students will not receive feedback on the grading of their exams.

Please note that exams may be re-scheduled to compensate for disruptions in the semester schedule and students are required to be available throughout the exam period including the scheduled Make-up Day.

A student with an exam conflict (or other circumstance that would justify rescheduling an exam under Mason policy), must notify the Instructor no later than 2 weeks prior to the scheduled exam; the student will be assigned to take the exam with another section of this course.

There are no opportunities for "extra credit" in this course. All students will be given the same opportunities to complete assigned work.

Students are expected to submit work as scheduled by the Instructor. Any assignment submitted after the due date-time but within 5 calendar days of it will be graded with a penalty of 10% of the available credit per day or part thereof. Any assignment submitted more than 5 calendar days late will not be graded. Exceptions to the submission time requirement may be made at the sole discretion of the Instructor.
Final grades will be posted to PatriotWeb, which is the only mechanism for students to obtain those grades. A student with a "hold" on his/her PatriotWeb account will be unable to access grades until the hold has been removed.

Schedule

This schedule is subject to revision before and throughout the course. Registered students should see Blackboard for the latest class schedule.

Important Dates

Please see the Fall 2021 Academic Calendar for important dates, including the last days to add and drop courses.

Religious Holidays

A list of religious holidays is published by University Life. Any student whose religious observance will conflict with a scheduled course activity must notify the Instructor at least 2 weeks in advance in order to make alternative arrangements.
## Lecture Content

<table>
<thead>
<tr>
<th>Lecture</th>
<th>Content</th>
</tr>
</thead>
</table>
| 1       | Topic 1. Introduction and Basic Security Concepts  
          | Topic 2. Basic Cryptography                        |
| 2       | Topic 3.1 Secret Key Cryptography – Algorithms  
          | Topic 3.2 Secret Key Cryptography -- Modes of Operations |
| 3       | Topics 3.3 Secret Key Cryptography -- Triple DES  
          | Topics 3.4 Secret Key Cryptography -- MAC           
          | Topic 4. Message Digest                            |
| 4       | Topic 5.1 Basic Number Theory -- Foundation of Public Key Cryptography |
| 5       | Topic 5.2 Public Key Cryptography                  |
| 6       | Topic 6.1 User Authentication                      |
| 7       | Topic 6.2 Design and Analysis of Authentication Protocols  
          | Review for mid-term exam                           |
| 8       | **Mid-term exam**                                  |
| 9       | Topic 7.1 Kerberos                                 
          | Topic 7.2 PKI                                      |
| 10      | Topic 8.1 IPsec: AH and ESP                        
          | Topic 8.2 IPsec: IKE                               |
| 11      | Topic 8.3 SSL/TLS                                  |
| 12      | Topic 8.4 Firewalls and IDS                        |
| 13      | Topic 8.5 Malicious Software                       |
| 14      | Review for final exam                              |
|         | **Final exam**                                     |

## Attendance Policy

Students are expected to complete any required preparatory work (including assigned reading – see Schedule above). Students in online sections are expected to join each online lecture session in real time and/or to promptly review the recording of the session such that they see the entire lecture no later than the end of the day following the day of the lecture.
Mason policy AP.3.10 requires students to take exams at the scheduled time and place, unless prior approval is granted by the student's academic dean or director. An unexcused absence from an exam will result in a score of zero (0) for that exam. Please note that exams may be re-scheduled by the Registrar to compensate for disruptions in the semester schedule and students are required to be available throughout the exam period including the scheduled Make-up Day.

Campus Notifications

Students are encouraged to subscribe to the Mason Alert system to receive notifications of campus emergencies, closings, and other situations that could affect class activities.

Each classroom has a poster explaining actions to be taken in different types of crisis. Further information on emergency procedures is available at the Emergency Management Web site. In the event of a possible emergency, students are encouraged to dial 911.

Classroom conduct

Students are expected to use the online tools provided solely for learning in relation to this course. Misuse of online tools may result in denial of access to those tools or other consequences under Mason policies.

Communications

Registered students will be given access to a Blackboard section for this course. Blackboard will used as the primary mechanism (outside of lectures) to disseminate course information, including announcements, lecture slides, homework and other assignments, and scores for homework and exams. Some announcements may be sent via Blackboard to students' Mason email accounts.

Communication with the Instructor on issues relating to the individual student only should be conducted using Mason email, via telephone, or in person - not in the public "Discussions" forums on Blackboard.

You must use your Mason email account for all email correspondence having anything to do with your work at Mason. Federal laws protecting your privacy rights require that we only communicate student information directly to students – and use of the university email system is our only way to validate your identity. You may forward your campus email elsewhere, but we can respond only to a Mason email account. Students are advised to use Blackboard, Tools, Send Email, Select Users to originate email messages to an Instructor.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided in Blackboard as a courtesy to students provided acceptable attendance is maintained.
All course materials (lecture slides, assignment specifications, etc) are published on Blackboard in Adobe® Portable Document Format (PDF). This allows users of most computing platforms to view and print these files. Microsoft® Word (or a compatible word processing application) is required for preparing assignments – it is available on computers in the Mason open labs.

Online sections will use several tools through Blackboard. Students are responsible for obtaining Internet access and a compatible platform. Appropriate computers are available on campus in open labs.

**Privacy**

Instructors respect and protect the privacy of information related to individual students. For information on student rights and privacy under the Family Educational Rights and Privacy Act of 1974 (FERPA) please see FERPA at Mason.

As described above, issues relating to an individual student will be discussed via email, telephone or in person. Instructors will not disclose protected information identifiable to an individual student with other students (or anyone without a need to know) without prior permission of the student.

Homework, quizzes, mid-term exams and other assessable work will be returned to each individual student directly by the Instructor (or by a faculty member, staff member, or Teaching Assistant designated by the Instructor, or via another secure method). Under no circumstances will a student's graded work be returned to another student.

Instructors, Teaching Assistants, and staff will take care to protect the privacy of each student's scores and grades.

**Academic Integrity**

All members of the Mason community are expected to uphold the principles of scholarly ethics.

The IT major has been designed to achieve several specific outcomes. One of those outcomes is: “An understanding of professional, ethical, legal, security, and social issues and responsibilities.”

Graduating students are bound by the ethical requirements of the professional communities they join. The ethics requirements for some of the communities relevant to IT graduates are available via the following links:

- [ACM Code of Ethics and Professional Conduct](https://www.acm.org/about/codes-of-conduct)
- [IEEE Code of Ethics](https://www.ieee.org/about/ethics)
- [EC-Council Code of Ethics](https://www.eccouncil.org/ethics)
On admission to Mason, students agree to comply with the requirements of the Mason Honor Code and System. The Honor Code will be strictly enforced in this course. Honor Code cases are heard by a panel of students – students who meet the requirements are encouraged to nominate themselves to serve on the Honor Committee.

Any use of the words or ideas of another person(s), without explicit attribution that clearly identifies the material used and its source in an appropriate manner, is plagiarism and will not be tolerated. The Instructor reserves the right to use manual and/or automated means (including such services as SafeAssign) to detect plagiarism in any work submitted by students for this course, and to direct Teaching Assistants and/or other faculty and/or staff members to do likewise in support of this course.

For this course, the following requirements are specified:

- All assessable work is to be prepared by the individual student, unless the Instructor explicitly directs otherwise.

- All work must be newly created by the individual student for this course for this semester. Any usage of work developed for another course, or for this course in a prior semester, is strictly prohibited without prior approval from the Instructor.

Students may seek assistance with assigned work (and are encouraged to do so if they feel the need), provided:

- The directions for the assigned work do not prohibit such assistance.

- Such assistance is explicitly acknowledged in the submitted work, clearly identifying the person(s) giving assistance and the nature of the assistance given.

- Any individual work to be submitted is prepared entirely and exclusively by the student submitting it. Students are expressly prohibited from sharing any individual assessable work for this course in any manner with other students (except students assigned as Teaching Assistants or Undergraduate Peer Mentors to this course and the student's section), unless all students involved have had their work graded and returned by the Instructor, or the Instructor has explicitly approved such sharing.

Another aspect of academic integrity is the free exchange of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. When using online tools to communicate, students are expected to follow the conventions of Netiquette. Mason values diversity: through the Office of Diversity, Inclusion, and Multicultural Education (ODIME), Mason seeks to create and sustain inclusive learning environments where all are welcomed, valued, and supported.

Students are encouraged to ask for clarification of any issues related to academic integrity and to seek guidance from the Instructor, other faculty members, academic advisors, or the Office for Academic Integrity.
Disability Accommodations

Disability Services works with disabled students to arrange for appropriate accommodations to ensure equal access to university services. Any student with a disability of any kind is strongly encouraged to register with Disability Services as soon as possible and take advantage of the services offered.

Accommodations for disabled students must be made in advance – Disability Services cannot assist students retroactively. Any student who needs accommodation should contact the Instructor no later than the first class.

If a student has an accommodation that allows the student to take an exam in the Disability Services Testing Center, the Instructor will determine the date and time of that exam – the student must not contact Disability Services to schedule the exam until the Instructor has advised the date and time.

Other Resources

Mason provides many useful resources for students – see Students - George Mason University. The following resources may be particularly useful:

- Volgenau School of Engineering - Computing Resources
- The Writing Center
- Academic Advising
- University Libraries
- Counseling and Psychological Services
- University Career Services

Students in online sections may benefit from these resources:

- Online Learning Resources
- University Libraries - Mason Online