

**University of Detroit Mercy**  
**College of Engineering and Science**  
**Department of Mathematics, Computer Science and Software Engineering**

**CSSE-5700 01 Applied Cryptology and Network Security (3 cr.)**  
**Winter 2016-2017**

**DESCRIPTION OF COURSE:** Block Ciphers and Data Encryption Standard, Advanced Encryption Standard, Other Symmetric Ciphers, Confidentiality Using Symmetric Encryption, Public-Key Cryptography And RSA, Key Management; Other Public-Key Cryptosystems, Message Authentication And Hash Functions, Hash And MAC Algorithms, Digital Signatures And Authentication Protocols, Authentication Applications, Transport Level Security, Electronic Mail Security, IP Security, Wireless Security, Projects.

**PREREQUISITES:** CSSE-1710 and MTH-1420

**PREREQUISITES BY TOPIC:** None

**REQUIRED TEXT:** Cryptology and Network Security: Principles and Practice, William Stallings, Prentice Hall, Sixth Edition, ISBN: 0-13-335469-5, 2014

**INSTRUCTOR:** Dr. Kevin Daimi, Room E324. Tel: 313-993-1060.

Email: [daimikj@udmercy.edu](mailto:daimikj@udmercy.edu)

Web page: <http://daimikj.faculty.udmercy.edu>

**OFFICE HOURS:** Tuesday and Thursday 02.00-3.00 pm. Or contact me to schedule an appointment.

**LECTURE:** TR 3.30-4.45 PM, Room E223.

**COURSE OBJECTIVE:** To introduce the concepts, techniques, standards, and methods of symmetric and public key encryption, digital signatures, and authentication, and their applications to computer and network security

**COURSE OUTCOMES:** Upon completion of the course, students will be able to:

1. Use advanced cryptographic techniques and algorithms and implement efficient key management techniques.
2. Protect networks at the transport level.
3. Secure wireless networks and internet protocols.
4. Provide electronic mail security.
5. Work in teams, apply ethics to their projects, and present them both orally and in writing
6. Use Cryptographic software tools

**COMPUTER USAGE:** Students will use JCrypTool, which can be downloaded from <https://www.cryptool.org/en/>.

**Schedule (Subject to Change):**

- Overview (Week 1)
- Classical Encryption Techniques (Week 1)
- Block Ciphers and the Data Encryption Standard (Week 2)
- Basic Concepts in Number Theory (Week 2)
- Advanced Encryption Standard (Week 3)
- Block Cipher Operation (Week 3)
- Pseudorandom Number Generation (Week 4)
- More on Number Theory (Week 4)
- Public Key Cryptology (Week 5)
- Other Public Key Cryptosystem (Week 5)
- Cryptographic Hash Functions (Week 6)
- Message Authentication Codes (Week 6)
- Digital Signature (Week 7)
- Key Management and Distribution (Week 7)
- User Authentication Protocols (Week 8)
- Transport Level Security (Week 8)
- Wireless Security (Week 9)
- Electronic Mail Security (Week 9)
- IP Security (Week 10)
- Exam, Term paper Presentations, Term Project Presentation/Discussion Weeks 11-14). See details below.

**COURSE ASSIGNMENTS:**

Term papers and projects will be presented by students. The dates and times for the presentations will be finalized by week 9 of the term.

Assignment	Topic Covered	Assign Date	Collect Date
Term Paper	Hardware Security	01/10/2017	03/02/2017
Term Project	Cryptographic Protocols for Vehicle Infotainment Systems	01/10/2017	03/30/2017

- *Students may suggest other projects subject to instructor approval*
- *Journal and conference papers used in preparing the Research Paper must be approved by the instructor by 01/19*
- *Project Plan and Paper Plan need be submitted on 01/26. Refer to the plan format for details*

## GRADING:

Term Paper	20%
Term Project	50%
Exam	30%

## EXAM SCHEDULE: (TENTITATIVE)

**Exam: Tuesday, March 28, 3.30-4.30 pm.**  
(All covered chapters + notes + handouts + papers + tools)  
**Paper Presentation: March 23, 30**  
**Term Project Presentation: April 4, 6, 11, 13, 18, 20**

## GRADING SCALE:

A 95-100, A- 90-94, B+ 85-89, B 80-84, B- 75-79,  
C+ 70-74, C 65-69, C- 60-64, D+ 55-59, D 50-54

## IMPORTANT DATES:

January 15	Last Day to Add a Class
January 15	Last Day to drop a Class without a "W"
January 16	Martin Luther King Jr. Holiday (No Classes)
February 01	Mid-Term Grades Due
March 06-11	Spring break
March 13	Advising for Fall Term Begins
March 20	Registration for Fall Term Begins
March 30	Last Day to Withdraw from Class
April 14-16	Easter Recess (university Closed)
April 25-29	Final Exam Week

## ATTENDANCE/PARTICIPATION

Students are expected to attend class on a regular basis and participate in the discussions. They are responsible for all the material presented therein. Formal attendance records will not be maintained; however, attendance is highly correlated with performance on the projects and the exams.

The instructor will attempt to make reasonable accommodations for students who miss a class due to illness, death in the family, or other legitimate reasons. However, students who are forced to miss several classes will have difficulty completing the course in a satisfactory manner. Make Up exams will only be given to students who miss an exam for legitimate reason (as defined above) and who notify the instructor in advance.

## CLASSROOM DECORUM

- Students are not allowed to talk to their classmates at any time unless permitted by the instructor.

- Cell phones are not allowed to be used and should be put away. They should be on silent mode.
- Computers can only be used to follow the PowerPoint slides of the class. Students can use their computers for other purposes when allowed by the instructor.
- Under normal road and weather conditions, students are allowed into the classroom no more than 5 minutes after the class starts.

## **CLASS CANCELLATION**

If a class is cancelled, students will be informed the day before or early morning of the day of the class. This applies to any other important messages.

## **ASSIGNMENT DEADLINES**

Enough time has been allocated for both the term papers and projects to be completed. If students follow instructions, they should be able to complete the assignments 1-2 weeks before the deadlines. Late papers and projects will not receive full credit. Unless otherwise specified, papers turned in late may lose as much as 10 points, and projects turned in late may lose as much as 20 points. Papers /projects may not be accepted at all if submitted a week after the deadline.

## **PROJECT/PAPER GROUP FORMATION**

Students can form their own teams for both the group paper and project. The instructor specifies the size of the groups. The instructor may make some changes to the groups if needed.

## **STUDENTS WITH DISABILITIES**

If you need an accommodation because of a disability, have emergency medical information to share, or if you need special arrangements in case the building must be evacuated, please contact:

Emilie Wetherington, Director  
 Disability Support Services.  
 McNichols Campus Library, Room 328  
 Email: [gallegem@udmercy.edu](mailto:gallegem@udmercy.edu)  
 Phone: 313-993-1158

It is very important for students to be proactive with regard to requesting their disability accommodations every semester. Students are encouraged to have open communication with their professors. However, it is a personal choice and never a requirement for students to disclose their disabilities to anyone except the Director of Disability Support Services, and only if they wish to request accommodations. You must be registered with Disability Support Services and your faculty must receive official notification from the DSS office before they can make arrangements for your accommodations.

## **IMPORTANT LINKS**

UDM Mission:

<http://www.udmercy.edu/mission/mission-vision/index.htm>

Engineering and Science College Mission:

<http://www.udmercy.edu/catalog/undergraduate2015-2016/colleges/eng-sci/>

Student Handbook:

<http://www.udmercy.edu/slo/office/handbook/index.htm>

Academic Integrity:

<http://www.udmercy.edu/catalog/graduate2016-2017/colleges/eng-sci/index.htm>

## **TITLE IX PROTECTIONS**

The University of Detroit Mercy is committed to promoting an environment which supports its educational mission and Jesuit and Mercy traditions. In addition, the University seeks to create a climate which preserves the safety and dignity of its members. In particular, the University views, with the utmost seriousness, offenses against an individual such as stalking, sexual harassment, inappropriate sexual touching, sexual assault and any other form of non-consensual sexual activity. The University experience includes learning to make wise choices. The decision-making process can be a challenge and an opportunity for students, faculty and staff. At the University of Detroit Mercy, choices are framed by an ethical and moral commitment to honesty, to the dignity of the individual and to responsibility to others.

**STATEMENT:** This is a tentative syllabus. Syllabus is subject to change.