Computer Science 480/697- Syllabus
Applied Cryptography

Instructor Information

Xiaohui Liang, PhD
Xiaohui.Liang@umb.edu
Phone (W): 617-287-6791
Office Location: McCormack Hall, 3rd floor, 201-24
Office Hours: Monday & Wednesday 2:00 PM - 3:30 PM or by appointment
Class room: Wheatley W02-0127
Class time: MoWeFr 13:00PM - 13:50PM

Note: The following link will assist you in forwarding your UMB email account to your personal account: Use this link. Throughout the semester, I will communicate with you via your UMB e-mail account. You may have e-mail redirected from your official UMass Boston address to another e-mail address at your own risk. The University will not be responsible for the handling of e-mail by outside vendors or by departmental servers.

Course Information

Course Title: Applied Cryptography

Credits: 3

Online Course: no

Description: This course aims to introduce the fundamental and practical knowledge of cryptography and its applications. This course covers diverse topics on cryptography and network security techniques including BITCOIN and BLOCKCHAIN, conventional encryption, asymmetric and symmetric cryptology, digital signatures, certificates, key exchange, key management, authentication, network access control, cloud computing security, electronic mail security, advanced crypto primitives. This course focuses on both theoretical concepts and practical applications of cryptanalysis and network security techniques.

Context: This course serves one of the electives in computer science.

Prerequisites: CS310 or permission of the instructor

Prerequisite Skills: None

Course Objectives: By fully participating in this course, you should be able to:

1. Understand the fundamental knowledge of the cryptographical technologies

2. Understand the security properties of the cryptographical technologies
3. Describe the cryptographical technologies
4. Identify the vulnerabilities of the cryptographical technologies
5. Apply the cryptanalysis skills to evaluate the cryptographical technologies
6. Examine the security and privacy challenges of cybersecurity problems
7. Identify the security properties of the cybersecurity problems
8. Apply the cryptographical technologies for cybersecurity problems
9. Explore new cybersecurity problems with solutions
10. Have hands-on experience in implementing security mechanisms

Core Competencies: The objectives for this course focus on the following core competencies:

1. Understand and describe the classical cryptographical technologies, such as RSA
2. Understand and identify the security properties of cryptographical technologies
3. Apply cryptanalysis skills to evaluate the cryptographical technologies
4. Have hands-on experience in implementing the cryptographical technologies

Required Assignments:

- Attendance: 5%
- Five assignments: 45% = 9% * 5
- Midterm exam: 20%
- For undergraduate students: Final exam (30%)
- For graduate student: Final exam (20%) + Final paper (10%)

Course Rubric:

Tests/Assignments/Deliverables	Number	Grade %
1. Assignments	**5**	**45%**
2. Midterm	**1**	**20%**
3. Final	**1**	**20%**
4. Final Paper (not required for undergraduate)	**1**	**10%**
5. Attendance	**1**	**5%**

Assignment Description:

Assignment 1 (9 points): Write a Python program to download the latest block from the public Blockchain, and verify the block is correct. The program needs to calculate the hash value from the given parameters and confirm that the calculated hash value is the same as the one downloaded from the public Blockchain. Partial points are given based on the number of correct calculations.

Assignment 2 (9 points): Write a Python program to mine new blocks from the puzzles with different parameters. Explain your observations on the computational costs when changing the parameters. The program needs to output the required parameters. Partial points are given based on the number of correct parameters.

Assignment 3 (9 points): Solve five modular arithmetic problems, and practice on the fundamental operations of the public cryptosystem. Partial points are given based on the number of solved problems.

Assignment 4 (9 points): Write a Python program to generate prime numbers and implement the RSA algorithm using the prime numbers. 4 points are given based on the prime generation program, and 5 points are given based on the RSA encryption and signature programs.

Assignment 5 (9 points): Prove two protocols are zero-knowledge protocol, i.e., proving they have completeness, soundness, and zero-knowledge properties. 1.5 points are given based on the explanation of each property (3 properties * 2 protocols).

Final Research Paper (10 points): All graduate students will write a research paper on a specific aspect of your studies. We will discuss crypto-related applications early in the semester and examine cryptographical technologies. Each student needs to find a crypto-related application (e.g., https, email, certificate, bitcoin, or authentication) and describe the security attacks towards the application, the desired security properties, and the adopted cryptographical technologies. The paper should be in 2-page letter size, single space, 12 pt, font Arial, Margin 1''. The paper needs to have sections introduction, related work, and discussion.

Course Policies:

Attendance – A roll call will be conducted at the end of each class. The attendance score is calculated as the number of the attended classes divided by the total number of the classes.

Assignments submission– For assignments, no late submissions are accepted unless you have made prior arrangements with me.

Exams – No makeup exam is provided unless you have made prior arrangements with me.

Grading

Grading: Grade type for the course is a whole or partial letter grade. (Please see table below)

Grading Policy for Undergraduate Students		
Letter Grade	**Percentage**	
A	90-100%	

	A-	87-89%	
	B+	84-86%	
	B	80-83%	
	B-	77-79%	
	C+	74-76%	
	C	70-73%	
	C-	67-69%	
	D+	64-66%	
	D	60-63%	
	F	<60%	

Note: the lowest passing grade for a graduate student is a "C". Grades lower than a "C" that are submitted by faculty will automatically be recorded as an "F".
Please see the Graduate Catalog or website for more detailed information on the University's grading policy.

Grading Policy for Graduate Students			
	Letter Grade	**Percentage**	**Quality Points**
	A	93-100%	4.00
	A-	90-92%	3.70
	B+	87-89%	3.30
	B	83-86%	3.00
	B-	80-82%	2.70
	C+	77-79%	2.30
	C	73-76%	2.00
	F	0-72%	0.0
	W	Received if withdrawal occurs before the withdrawal deadline.	N/A
	AU	Audit (only permitted on space-available basis)	N/A
	NA	Not Attending (student appeared on roster, but never attended class. Student is still responsible for tuition and fee charges unless withdrawal form is submitted before deadline. NA has no effect on cumulative GPA.)	N/A

Required
Text(s): First book: Mihir Bellare and Phillip Rogaway, Introduction to Modern Cryptography, 2005.
Available at: http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf

Second book: Shafi Goldwasser and Mihir Bellare, Lecture Notes on Cryptography, 2008.
Available at: https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

Third book: W. Stallings. Cryptography and Network Security: Principles and Practices

(7th edition). Prentice Hall, 2016, ISBN-13: 978-0134444284
Available at: http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf

Recommended
Texts: W. Mao, Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2003, ISBN: 0130669431

D. Stinson, Cryptography: Theory and Practice (Third Edition). CRC Press, 2005, 978-1584885085

Course Schedule

Week 1:

Core Topic(s):	1. Introduction to course and introduction to security: security goals and security attacks 2. Where we can find applied crypto in our daily lives? Why we use them? 3. Introduction to mobsps server for projects
Learning Objectives:	1. Understand the fundamental knowledge of the cryptographical technologies 2. Understand the security properties of the cryptographical technologies 3. Examine the security and privacy challenges of cybersecurity problems
Reading Assignment	Section 1 of the first book and section 1 of the second book

Week 2:

Core Topic(s):	1. Hash function, and python program to generate hash values 2. Digital signature, security properties, and python program to generate digital signature 3. Application: Blockchain. How to verify a block?
Learning Objectives:	1. Understand the fundamental knowledge of the cryptographical technologies 2. Understand the security properties of the cryptographical technologies 3. Describe the cryptographical technologies 4. Have hands-on experience on implementing security mechanisms
Reading Assignment	Sections 6,7,12 of the first book and Section 8 of the second book.
Assignment(s):	Assignment 1: Write a Python program to download the latest block from

Due Date:	the public blockchain, and verify the block is correct. Due in two weeks

Week 3:

Core Topic(s):	1. Bitcoin. What is the cryptocurrency? What security needs to be guaranteed? 2. Blockchain from user's perspective. Transactions, blocks, and blockchains. 3. Blockchain from miner's perspective. Proof of work, fork problem, and consensus.
Learning Objectives:	1. Understand the fundamental knowledge of the cryptographical technologies 2. Understand the security properties of the cryptographical technologies 3. Describe the cryptographical technologies
Reading Assignment	Where Is Current Research on Blockchain Technology? A Systematic Review, 2016

Week 4:

Core Topic(s):	1. Blockchain: distributed network with self-optimization and self-healing properties. 2. Other Blockchain applications: smart contract and IoT 3. Power of hash and signature for building blockchain
Learning Objectives:	1. Examine the security and privacy challenges of cybersecurity problems 2. Identify the security properties of the cybersecurity problems 3. Have hands-on experience on implementing security mechanisms
Reading Assignment	Majority Is Not Enough: Bitcoin Mining Is Vulnerable, Communications of the ACM 2018
Assignment(s): Due Date:	Assignment 2: Write a Python program to mine new blocks from the public puzzles with different parameters. Explain your observations on the computational costs when changing the parameters. Due in three weeks

Week 5:

Core Topic(s):	1. Blockchain summary with Q&A 2. Perfect secrecy. What is ideal case for encryption? 3. Perfect secret cryptosystem and its properties.

Learning Objectives:	1. Understand the fundamental knowledge of the cryptographical technologies 2. Understand the security properties of the cryptographical technologies 3. Describe the cryptographical technologies 4. Identify the vulnerabilities of the cryptographical technologies 5. Apply the cryptanalysis skills to evaluate the cryptographical technologies
Reading Assignment	https://bitcoin.org/en/faq#general

Week 6:

Core Topic(s):	1. Symmetric cryptosystem: confusion and diffusion, DES, and AES 2. Encryption mode and analysis: ECB, CBC, and Counter. Experiments to test block size 3. Pros and cons of symmetric cryptosystem
Learning Objectives:	1. Describe the cryptographical technologies 2. Identify the vulnerabilities of the cryptographical technologies 3. Apply the cryptanalysis skills to evaluate the cryptographical technologies
Reading Assignment	Sections 2-5 of the first book and Section 4,6 of the second book

Week 7:

Core Topic(s):	1. Mid-term review 2. Mid-term exam 3. Number theory: Group, subgroup, cyclic group
Learning Objectives:	1. Understand the fundamental knowledge of the cryptographical technologies 2. Have hands-on experience on implementing security mechanisms
Reading Assignment	Section 9-10 of first book.
Assignment(s): Due Date:	Assignment 3: Solve modular arithmetic problems, and practice on the fundamental operations of the public cryptosystem. Due in two weeks

Week 8:

Core Topic(s):	1. Number theory: modular operator and arithmetic operations

	2. Great common divisor, and Euclid and Extended Euclidean algorithms 3. Euler Totient Function, Fermat's little theorem, and Euler's theorem
Learning Objectives:	1. Understand the fundamental knowledge of the cryptographical technologies 2. Understand the security properties of the cryptographical technologies
Reading Assignment	Section 9-10 of first book.

Week 9:

Core Topic(s):	1. Public key cryptosystem: Advantage and computational assumption, factoring challenge 2. RSA encryption and its security analysis 3. RSA signature and its security analysis
Learning Objectives:	1. Understand the security properties of the cryptographical technologies 2. Describe the cryptographical technologies 3. Identify the vulnerabilities of the cryptographical technologies 4. Apply the cryptanalysis skills to evaluate the cryptographical technologies 5. Have hands-on experience on implementing security mechanisms
Reading Assignment	Section 11 of the first book and Section 7 of the second book.
Assignment(s): Due Date:	Assignment 4: Write a Python program to generate wanted prime numbers and implement the RSA algorithm using the prime numbers. Due in three weeks

Week 10:

Core Topic(s):	1. Discrete logarithm problem and assumption 2. ElGamal encryption and signature 3. Diffie-Hellman key exchange
Learning Objectives:	1. Understand the security properties of the cryptographical technologies 2. Describe the cryptographical technologies 3. Identify the vulnerabilities of the cryptographical technologies 4. Apply the cryptanalysis skills to evaluate the cryptographical technologies
Reading Assignment	Section 11 of the second book

Week 11:

Core Topic(s):	1. Secret sharing and Shamir's 2. Proactive secret sharing 3. Verifiable secret sharing
Learning Objectives:	1. Understand the security properties of the cryptographical technologies 2. Describe the cryptographical technologies 3. Identify the vulnerabilities of the cryptographical technologies 4. Identify the security properties of the cybersecurity problems 5. Apply the cryptographical technologies for cybersecurity problems
Reading Assignment	Section 12 of the second book

Week 12:

Core Topic(s):	1. Commitment 2. Zero-knowledge proof
Learning Objectives:	1. Understand the security properties of the cryptographical technologies 2. Describe the cryptographical technologies 3. Apply the cryptanalysis skills to evaluate the cryptographical technologies 3. Identify the security properties of the cybersecurity problems 4. Have hands-on experience on implementing security mechanisms
Reading Assignment	Section 12 of second book
Assignment(s): Due Date:	Assignment 5: Prove two protocols are zero-knowledge protocol, i.e., proving they have completeness, soundness, and zero-knowledge properties. Due in three weeks

Week 13:

Core Topic(s):	1. Review of hash and signature on Blockchain 2. Review of symmetric cryptosystem 3. Review of public key cryptosystem
Learning Objectives:	1. Apply the cryptanalysis skills to evaluate the cryptographical technologies 2. Apply the cryptographical technologies for cybersecurity problems

	3. Explore new cybersecurity problems with solutions

Week 14:

Core Topic(s):	1. Review of DH key exchange, secret sharing, and zero-knowledge proof 2. Practice on numbers 3. Practice on programs
Learning Objectives:	1. Apply the cryptanalysis skills to evaluate the cryptographical technologies 2. Apply the cryptographical technologies for cybersecurity problems 3. Explore new cybersecurity problems with solutions

Methods of Instruction

Methods:

- Lecture slides via projector
- Handwriting on blackboard
- Live demo on Python programs
- In-class discussion
- Online discussion in UMB Blackboard system

Accommodations

The University of Massachusetts Boston is committed to providing reasonable academic accommodations for all students with disabilities. This syllabus is available in alternate format upon request. Students with disabilities who need accommodations in this course must contact the instructor to discuss needed accommodations. Accommodations will be provided after the student has met with the instructor to request accommodations. Students must be registered with the Ross Center for Disability Services, CC UL 211 (617.287.7430) before requesting accommodations from the instructor. http://www.umb.edu/academics/vpass/disability/. After registration with the Ross Center, a student should present and discuss the accommodations with the professor. Although a student can request accommodations at any time, we recommend that students inform the professor of the need for accommodations by the end of the Drop/Add period to ensure that accommodations are available for the entirety of the course.

Academic Integrity and The Code of Student Conduct

It is the expressed policy of the University that every aspect of academic life not only formal coursework situations, but all relationships and interactions connected to the educational

process shall be conducted in an absolutely and uncompromisingly honest manner. The University presupposes that any submission of work for academic credit indicates that the work is the student's own and is in compliance with University policies. In cases where academic dishonesty is discovered after completion of a course or degree program, sanctions may be imposed retroactively, up to and including revocation of the degree. Any student who reasonably believes another student has committed an act of academic dishonesty should inform the course instructor of the alleged violation. These policies are spelled out in the Code of Student Conduct. Students are required to adhere to the Code of Student Conduct, including requirements for academic honesty, as delineated in the University of Massachusetts Boston Graduate Catalogue and on their Website and in relevant program student handbook(s) or websites. UMB Code of Student Conduct
You are encouraged to visit and review the UMass website on Plagiarism*:* Plagiarism Prevention & Awareness: Home

Other Pertinent and Important Information

You are advised to retain a copy of this syllabus in your personal files for use when applying for future degrees, certification, licensure, or transfer of credit.