Applied Cryptography Course Outline

Course Title	**Applied Cryptography and Cybersecurity**
Description	Students in this course are introduced modern cybersecurity, security engineering and modern cryptology. It covers basic building blocks in computer security such as block ciphers, stream ciphers, and public-key encryption, as well as mutual authentication such as cryptographic hash, message authentication codes and digital signatures. It also introduces fundamental principles and engineering in cybersecurity such as CIAAA, access control, identification management, policies, procedures and awareness, physical security, perimeter defenses, network defense, data and application defenses, assessment and audits, and other latest developments. Class discussion, lab and teamwork are emphasized throughout the semester. 3 credits
Objective	Students will (1) develop an understanding the importance of codes, ciphers, and algorithms, (2) survey various classical ciphers and understand their weakness, (3) understand the working mechanism of stream cipher and block cipher, and their attacks (4) comprehend hash functions and related applications including attach techniques (5) describe public key systems and public key attacks (6) utilize various tools to do cryptanalysis (7) broaden crypto to a system engineering view on security and analysis real world cases analytically and systematically. (8) conduct internet and literature search for any latest development in cybersecurity
Prerequisite	Students shall have knowledge and understanding from Discrete Structures, Programming, Number theory, and Linear algebra such as modular operations, Group, Field and Matrix. Concepts form Computer architecture and network are also helpful.
Instructor	Dr. Z Chen, Professor Email: zxchen@ieee.org wechat: zchenny
Time	Beijing Time: 9/19 – 12/10/2022, B19-1: **M**: 08:20AM – 09:50AM, **W**: 10:05AM – 11:35AM
Office Hour	By appointment – use zoom session
Course Reference Materials	**Main Text in English:** 1. (Smart) Cryptography Made Simple, Nodel Smart, 2016, ISBN : 978-3-319-21935-6. Online reading / download from https://link.springer.com/book/10.1007/978-3-319-21936-3#toc **Main Reference book in Chinese** 2. (Stalling) William Stalling, Cryptography and Network Security, Principles and Practice, 5th Ed. https://icourse.club/uploads/files/d17a60cf3d2b8455de607d1449f47e49498b06f2.pdf **Other references** 3. (Joy) The Joy of Cryptography, Mike Rosulek, 2021, https://joyofcryptography.com/ online reading or download

	4. (Stamp) Applied Cryptanalysis: Breaking Ciphers in the Real World, Mark Stamp, Richard M. Low, John Wiley & Sons, 2007, ISBN: 978-0-470-14876-1, online pdf 5. (Schneier) Applied Cryptography, Protocols, Algorithms and Source Code in C, Bruce Schneier, 2nd Ed 6. (Pass) A Course in Cryptography, Rafael Pass and Abhi Shelat, 2010, https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf 7. archive.keyllo.com/L-编程/Code-现代密码学—原理与协议.pdf
Modality Logistics	1. Due to government guideline and travel restriction, the course modality is online and synchronized and asynchronized) 2. Course materials are posted inside **Blackboard (BB)**, and assignments (quizzes and projects) are conducted in the BB as well. 3. Online Sync is via zoom: https://mercy.zoom.us/j/99742935007?pwd=V3pVR2xSVmU3SER0RWhkN3hCeEhoZz09 Meeting ID: 997 4293 5007, Passcode: 168430 a. Need a quiet place like classroom b. Need a computer having camera enabled for showing face during the class c. Mobile devices are not suitable for the learning, only for emergency use 4. The class uses wechat group for short announcement as an alert.
Course Evaluation & points	The class is assessed by projects, quizzes, final exam and participation. They are posted in BB. Usually there are no late work unless a written excuse is provided. Projects 30 (3 projects) quizzes 30 (11 quizzes) End-term test 30 Class Q &A 10
Honesty	Academic honesty is highly valued. Students must always submit work that represents their original words or ideas. If any words or ideas used do not represent their original words or ideas, they must cite all relevant sources and make clear the extent to which such sources were used. Words or ideas that require citation include, but are not limited to, all hard copy or electronic publications, whether copyrighted or not, and all verbal or visual communication when the content of such communication clearly originates from an identifiable source. In particular, – **Do not to turn in the work of others** – **Do not give others the work to use as their own** – **Do not plagiarize from others (published or not)** – **Do not try to deceive the instructors** Remember, it does not prevent them from discussing any ideas and homework with their classmates and others. Such intellectual exchange is encouraged.
Students With Disabilities	Shanghai Jianqiao University is committed to achieving equal educational opportunities and full participation for persons with disabilities. Persons with disabilities who may need accommodations are encouraged to discuss with their advisors and instructors.

Contents and Schedule

Week #	Start Date	Subjects	Topics	Tasks
1	9/18	Course outline Course Logistics Crypto System	Student learning outcome Course arrangement • Crypto Terminology • Crypto (Encryption) Scheme • Key • Kerckhoff's Principle • Security Experiment • Provable Security • One time Pad	Joy-Chapter 1 Lecture Notes Quiz
2	9/25	Classical Encryption	• History of Cryptography • Substitution • Proposition Statistical Analysis	1. Stamp-Chap1.4 2. Smart-Chapt 7 3. Review Slide Quiz
3	10/02	Mechanical Encryption	• Machine Crypto • Enigma Machine • Rotors • Reflector • Stecker • Keys • Demo • Bombe known plaintext attacks	Smart-8 Stamp-chapter 2 Quiz Proj1-Enigma
4	10/09	Math Foundation	• Math Foundations • Modula Operations • Cyclic Group • Field • The extended Euclidean Algo • Chinese Remainder Theorem • Prime • Discrete Logarithm	Lecture Notes Smart-Part I Quiz
5	10/16	Security Principles	• Defining Security • CIA • Pseudo Random • Notions of security of encryption schemes • One way function • Security Notion • Authentication	Smart-11 Quiz

			• Bit Security • Computational Models • Types of attacks	
6	10/23	Garbled Circuits	• Garbled Circuits • Construction • Yao's Protocol • Evaluation • Secure Multi-party Comm	Smart-Chapter22 Quiz Proj2 - Garbled Circuits
7	10/30	Stream Cipher	• Stream Cipher • Linear Feedback Shift Registers • OFB and CFB • RC4 • Salsa20 • Chacha20	Smart-Chapter12 Quiz
8	11/06	Block Cipher	• Block Cipher • AES	Smart-chapter13 Lecture Notes Quiz
9	11/13	Public Key	• Public Key • RSA Cryptosystem • Key Management • Public Key Encryption	Smart-chapter15,16 Lecture Notes Quiz
10	11/20	Modes	• Mode of operations • ECB • CBC • CTR • OFB • CFB • GCM	Smart-chapter13 Lecture Notes Quiz
11	11/27	Mutual Authentication	• Cryptographic Hash Functions • Message Authentication Codes • Digital signature • Signature Schemes • Secure Signature Schemes • Plain RSA Signature • RSA FDH • RSA-PSS	Smart-chapter14,16 Lecture Notes Quiz
12	12/04	Blockchain	• Diffie Hellman Key Exchange • Blockchain Consensus	Lecture Notes Smart-Chapter 3.3/15,16 Quiz Proj3-zkSNARK

		MISC	• Zero knowledge • Interactive • Non-interactive • Proof • Commitment • Secure Multiparty Computation	
		Final exam		

Academic Integrity For Reference

Academic integrity is the pursuit of scholarly activity in an honest, truthful and responsible manner. Students are required to be honest and ethical in carrying out all aspects of their academic work and responsibilities.

Dishonest acts in a student's academic pursuits will not be tolerated. Academic dishonesty undermines the College's educational mission as well as the student's personal and intellectual growth. In cases where academic dishonesty is uncovered, the College imposes sanctions that range from failure of an assignment to suspension and expulsion from the College, depending on the severity and reoccurrence of the case(s).

Examples of academic dishonesty include, but are not limited to, cheating, plagiarism, obtaining unfair advantage, and falsification of records and official documents.

Cheating is the unauthorized use or attempted use of material, information, notes, study aids, devices, or communication during an academic exercise. Examples of cheating include, but are not limited to:

- Copying from another student during an examination or allowing another to copy your work
- Providing assistance to acts of academic misconduct
- Unauthorized collaboration on a take-home assignment or examination
- Using notes during a closed book examination
- Submitting another's work as your own
- Unauthorized use during an examination of any electronic device, such as cell phones, computers, or internet access to retrieve or send information
- Allowing others to research or write assigned papers for you or to complete your assigned projects

Plagiarism is the act of presenting another person's idea, research or writings as your own. Examples of plagiarism include, but are not limited to:

- Copying another person's actual words or images without the use of quotation marks and citations attributing the words to their source
- Presenting another person's ideas or theories in your own words without acknowledging the source
- Engaging in plagiarism, via the Internet or other web-based or electronic sources, which includes (but is not limited to) downloading term papers or other assignments and then submitting that work as one's own, or copying or extracting information and then pasting that information into an assignment without citing the source, or without providing proper attribution.

Obtaining unfair advantage is any action taken by a student that gives that student an unfair advantage, or through which the student attempts to gain an unfair advantage in his/her academic work over another student.
Examples of obtaining an unfair advantage include, but are not limited to:

- Gaining advance access to examination materials by stealing or reproducing those materials
- Retaining or using examination materials which clearly indicate the need to return such materials at the end of the examination
- Intentionally obstructing or interfering with another student's work

Falsification of Records and Official Documents include, but are not limited to, acts of forging authorized signatures, or falsifying information on an official academic record.

Consequences for Policy Violation
A student who is found to be dishonest in submission of his or her academic assignments or other work, or in carrying out his or her academic responsibilities may, at minimum, receive a zero for the submitted assignment, may receive a failing grade for the course, or may be subject to further suspension or expulsion from the College depending on the severity of the offense(s). Regardless, all incidents of academic dishonesty will be reported to the Academic Unit Head and School Dean, and may be retained by the College in the student's records.

Reporting
A faculty member who suspects that a student has committed a violation of the Academic Integrity Policy shall review with the student the facts and image circumstances of the suspected violation whenever feasible. Thereafter, a faculty member who concludes that there has been an incident of academic dishonesty sufficient to affect the student's final course grade shall report such incident on the Student Violation of the Academic Integrity Policy Form (located on Mercy Connect under the faculty tab) and submit it to the Dean of the appropriate School. The Dean shall update the Student Violation of the Academic Integrity Policy Form after a suspected incident has been resolved to reflect that resolution. Unless the resolution exonerates the student, the Student Violation of the Academic Integrity Policy Form will be placed in a confidential academic integrity file created for the purposes of identifying repeat violations, gathering data, and assessing and reviewing policies.

Academic Sanctions
If a faculty member believes that the appropriate sanction is academic in nature (e.g., a reduced grade) and the student does not contest either his/her guilt or the particular reduced grade that the faculty member has chosen, then the student shall be given the reduced grade, unless the Dean decides to seek a disciplinary sanction. The reduced grade may apply to the particular assignment where the violation occurred or to the course grade, at the faculty member's discretion. A reduced grade may be an "F", or another grade that is lower than the grade that the student would have earned but for the violation. If a faculty member determines that a student has committed an act of cheating or plagiarism, and the student withdraws from the course, that student will receive an "FW" for the course regardless of the time of withdrawal. The faculty member shall inform the Dean of the resolution via email and the Dean shall update the applicable Student Violation of the Academic Integrity Policy Form to reflect that resolution. In a case where a student admits to the alleged academic dishonesty but contests the academic sanction imposed by the faculty member, or in a case where a student denies the academic dishonesty, the student may appeal to the College's Undergraduate or Graduate Academic Appeals Committee.

Judicial Sanctions
In a case where the allegation of cheating or plagiarism is severe, or where the student has a history of violations of the Academic Integrity Policy which conduct warrants suspension or expulsion from the College, the school Dean shall impose a sanction in addition to or in lieu of academic sanctions, as he/she deems is warranted under the circumstances. If the student contests the judicial sanction imposed, he/she may appeal to the Undergraduate or Graduate Academic Appeals Committee.

Appeals
Appeals to the Undergraduate or Graduate Academic Appeals Committee shall be made within 7 business days of receipt of notice of the academic or judicial sanction. All parties will be permitted to participate and are permitted to submit any documentation they believe is necessary including written statements and documentary evidence. The Undergraduate or Graduate Academic Appeals Committee shall convene within two weeks of the filing of the appeal submission. The Undergraduate or Graduate Academic Appeals Committee shall issue a written decision of its finding within 7 business days of convening and shall send copies of its decision to the accused student, the faculty member and the appropriate Dean for

archiving in the student's confidential academic integrity file. If the Undergraduate or Graduate Academic Appeals Committee finds that no violation occurred, the Dean shall remove all material relating to that incident from the student's confidential academic integrity file and destroy the material.

This policy applies to all course delivery modalities including online courses.