Course Syllabus

Applied Cryptography

Fall 2025

Instructor

Prof. Z Chen, PhD, CISSP
Use email: zxchen@ieee.org or wechat: zchenny. Class wechat group is set. Please follow it closely.

Semester

Class Period: 9/8(M) – 11/29/2025 (M), Holidays: TBA
Zoom Sessions: M 8:20 – 11:35 AM (Beijing Time)
link: https://mercy.zoom.us/j/96324612888?pwd=onKs0mESSE1GwgQqzm2wqOyN8azaLl.1

Catalogues Description (new)

This course introduces the concepts and practical applications of cryptography and computer security. Topics include core primitives of applied cryptography such as block ciphers, stream ciphers, public-key encryption, cryptographic hashes, message authentication codes, and digital signatures. Students will also study randomness, key establishment protocols and public key infrastructure. The mathematical foundations—primarily number theory, group theory, and abstract algebra—are introduced as needed, including modular arithmetic, primality testing, fields, and related structures. The course emphasizes an applied perspective, integrating laboratory exercises, class discussions, and team-based projects throughout the semester.
3 credits

Course Objectives

This course is designed to provide a comprehensive overview of cryptography, tailored for security professionals and working practitioners, emphasizing a balance between theoretical concepts and applied approaches. The objectives are:

1. Develop a deep understanding of modern Cryptography, including its primitives, foundational principles and key areas of application.
2. Analyze and evaluate cryptographic algorithms and protocols, understanding their design, functionality, and security properties.
3. Assess the performance, security, and integration of cryptographic methods within complex security systems and solutions.
4. Understand the significance of mathematical foundations, including number theory, algebra, modular arithmetic, fields, and matrices, in establishing cryptography as a rigorous and robust scientific discipline.
5. Apply cryptographic techniques to real-world scenarios, addressing practical challenges and implementation considerations in contemporary security environments.

Student Learning Outcome

Upon completing this course, students should be able to do and demonstrate the followings outcomes.

1. Understand the importance of codes, ciphers, and algorithms.
2. Survey various classical ciphers and recognize their weaknesses.
3. Explain the mechanisms of stream ciphers and block ciphers, and their common attacks.
4. Comprehend hash functions and related applications, including attack techniques.
5. Describe public key systems and their vulnerabilities.
6. Apply cryptanalysis tools effectively.
7. Extend cryptography to a systems-engineering view of security and analyze real-world cases systematically.
8. Conduct internet and literature searches to identify the latest developments in cybersecurity.

Prerequisite

The following prerequisites are recommended to students attending this class.

- Understanding mathematical definitions, concepts, proofs, and notions of logic, set theory, number theory, abstract algebra, probability, and statistics.
- knowledge of basic algorithm analysis and complexity theory
- Familiarity with the Python programming language. Class projects are using jupyter notebook.

Course Main Materials

- (English, Smart) Cryptography Made Simple, Nogel P 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
- (Chinese Translation, Stalling) William Stalling, Cryptography and Network Security, Principles and Practice, 5th Ed. https://icourse.club/uploads/files/d17a60cf3d2b8455de607d1449f47e49498b06f2.pdf
- We may refer to others listed inside Bibliography section.

Assessment

The class is assessed by active participation (with oral discussion), quizzes, written practice, and hands on projects. Usually, no late work unless an arrangement was made or a written excuse is provided.

Point distributions

10% Active Participation.

20% Class Quizzes and Assignments.

50% Individual and team projects

20% One exam (essay)

Class Logistics

- Zoom Attendance is recorded.
- We will use the course management platform https://fanya.chaoxing.com/portal and ask Prof. YU, Fan and any access and test related questions.
- WeChat class group will be used for class announcement and notice.
- Office hour: individual zoom session by appointment.
- Zoom and zoom etiquette
  - Personal Computer with camera. Smart phones are for emergencies only.
  - Find a quiet corner with headphone.
  - Show face or set up face photo in zoom settings plus official name.
  - Take notes and ask questions.
- Personal Computer is being used for the class projects and assignments.

Success Tips

- **Be disciplined.** Consistent, focused effort is key to succeeding in this class.
- **Read carefully.** Avoid skimming—cryptography concepts require time to digest. Read line by line, take notes, and list questions as you go.
- **Use online and AI resources wisely.** The internet can be a valuable learning repository, and AI assistants may be used in this class. However, always verify information critically and never submit AI-generated answers without your own curation and investigation.
- **Maintain academic honesty.** Submit only work that reflects your own words and ideas. If you use others' words or ideas, cite them clearly, regardless of whether they are from print, online, verbal, or visual sources. This includes:
  - Do not submit others' work as your own.
  - Do not provide your work for others to use as their own.
  - Do not plagiarize from any source (published or unpublished).
  - Do not attempt to deceive the instructors.
- **Collaborate ethically.** Discussing ideas and homework with classmates is encouraged, as long as the work you submit is your own.

Students W/ Disabilities

Shanghai Jianqiao University is committed to achieving equal educational opportunities and full participation for people with disabilities. People with disabilities who may need accommodation are encouraged to discuss with their advisors and instructors.

Bibliography

1. (Joy) The Joy of Cryptography, Mike Rosulek, 2021, https://joyofcryptography.com/ online reading or download
2. (Aumasson) Serious Cryptography: A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson, 2017, online pdf
3. (EKR) A Pragmatic Introduction to Secure Multi-Party Computation, David Evans, Vladimir Kolesnikov, Mike Rosulek, 2022
4. https://securecomputation.org/docs/pragmaticmpc.pdf
5. https://www.coursera.org/learn/crypto.
6. Various online videos
7. ***A Course in Cryptography***, Heiko Knospe, American Mathematical Society, 2017, LCCN 2019011732 | ISBN 9781470450557
8. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*, by John F Dooley, Springer, August 24, 2018, ISBN-13: 978-3319904429, ISBN-10: 3319904426
9. *A Graduate Course in Applied Cryptography, by* Dan Boneh and Victor Shoup, v0.5, Jan 2020, downloadable at http://toc.cryptobook.us/
10. *Cryptography and Network Security: Principles and Practice, 7th edition, by William Stallings, 2017, Pearson, ISBN13: 978-0-13-444428-4*
11. *Cryptography: An Introduction by Smart, N. McGraw-Hill, 2002 (ISBN: 0077099877)*
12. *Network Security, Private Communication in a Public World, by Kaufman, Perlman, Speciner. 2nd Ed, Prentice-Hall. 2002 ISBN 0-13-046019-2.*
13. *Hacking Exposed by McClure, Scambray, Kurtz. 4th Ed, McGraw-Hill. 2003. ISBN 0072227427.*
14. *Handbook of Applied Cryptography by A. Menezes, P. Van Oorschot, S. Vanstone. CRC Press ISBN: 0-8493-8523-7 (downloadable at http://cacr.uwaterloo.ca/hac/*
15. *A Graduate Course in Applied Cryptography by D. Boneh & V. Shoup, downloadable at http://toc.cryptobook.us/*
16. *Introduction to Modern Cryptography (2nd edition) by J. Katz and Y. Lindell. CRC Press 2014 ISBN-13: 978-1466570269, check http://toc.cryptobook.us/*
17. *Cryptanalysis, A Study of Ciphers and Their Solution, by Helen F. Gaines, 1989*
18. *The Code Book, The Secrets Behind Codebreaking, by Simon Singh|, August 12, 2003*
19. *Decrypted Secrets, Methods and Maxim of Cryptology, by Friedrich L. Bauer, 3rd rev. and updated ed. Edition, Springer, 2007, ISBN-13: 978-3540245025, ISBN-10: 3540245022*
20. *Elementary Cryptanalysis, by Abraham Sinkov, Todd Feil, 2009*
21. *Heuristic Cryptanalysis of Classical and Modern Ciphers, by Ho Yean Li, 2015*
22. *Cryptanalysis of Number Theoretic Ciphers (Computational Mathematics) by Samuel S. Wagstaff Jr. 2003, Taylor and Francis, LLC*
23. *Algorithmic Cryptanalysis, Antoine Joux, CRC Press, Jun 15, 2009*
24. *Applied Cryptanalysis: Breaking Ciphers in the Real World, by Mark Stamp, Richard M. Low, John Wiley & Sons, Jun 15, 2007, ISBN: 978-0-470-14876-1*
25. *Modern Cryptanalysis: Techniques for Advanced Code Breaking, Christopher Swenson, John Wiley & Sons, Mar 17, 2008*
26. *https://en.wikipedia.org/wiki/Cryptanalysis*
27. *Shannon, C.E., Communication Theory of Secrecy Systems, BSTJ 28: 4. October 1949, https://ia802703.us.archive.org/2/items/bstj28-4-656/bstj28-4-656.pdf*

Weekly Course Arrangement (subject to change)

wk	Module	Contents	Activity

1	Crypto System Overview
	
	Course Outline
		• Good or bad guys
		• Cryptosystem for Secure Communication
		• Cryptosystem for Secure Data Storage
		• Crypto terminology
		• Security through/by Obscurity
		• Security by Moving Target Defense (MTD)
		• Kerckhoff's Principle
		• OTP
		• Cryptographic Primitives
		  ○ Stream ciphers
		  ○ Block Ciphers
		  ○ Public Key Scheme
		  ○ Hash
		  ○ Message Authentication Code (MAC)
		  ○ Digital Signature
		• Primitive Constructs
		  ○ Pseudo-random Generators (PRGs)
		  ○ Pseudo-random Functions (PRFs)
		  ○ Pseudo-random Permutations (PRPs)
		  ○ One-Way Functions (OWFs)
		  ○ Trapdoor One-Way Functions (TOWFs)
		  ○ Randomness
		• Homomorphic Encryption Scheme
		• Plaintext Aware Encryption Scheme
		• Key Encapsulation Mechanisms
		• Wisdom from Cryptographers
		
		Course Logistics
		Class Hello (no recording)
			▪ Read and sign off the course outline
			
			▪ Review with the slides.
			▪ Read the references listed in the slides.
			▪ Prepare for the class Quiz

2	Classical and Mechanical Encryption	• Simple Substitution
		• Poly-Alphabetic Substitution
		• Affine Cipher
		• Vigenère Cipher
		• Transposition Cipher
		• Scytale
		• Columnar Transposition
		• Statistical Analysis
		• Index of Coincidence
		• Enigma Machine
		  ○ Rotors
		  ○ Reflector
		  ○ Stecker
		  ○ Keys
		  ○ Demo
		  ○ Bombe known plaintext attacks
			▪ Review with the slides.
			▪ Read the references listed in the slides.
			▪ Do the class quiz
			▪ Work on the individual project 1 and is due in 3 weeks.

3	Overview – Security	• Security of a cryptosystem
		• NP Hard
		• Attack Complexity
		• Breaking a cryptosystem
		• Probably safe or fine notions
		• Secure and insecure cryptosystem
		• Cryptography and CIA
		• Cryptographic Attack Model
		• Security Game (Framework)
		  ○ Setup
		  ○ Why Security Game (Significant)
		  ○ Properties of the Security Attack Game
		  ○ Adversary's Advantage
		• IND-EAV (Eavesdropping)
		• IND-CPA (Chosen plaintext attack)
		• IND-CCA (Chosen-ciphertext attack)
		• Pseudorandom Generators, Functions, permutations
		• Forward Security and Backward Security
		• Wisdom - think like cryptographer
		• One time Pad – Perfect Security (self-study)
			▪ Watch the class video.
			▪ Review with the slides.
			▪ Read the references listed in the slides.
			▪ Do the class quiz

4	Mathematical Foundations	• Divisibility and modular operations • Modular Inverse • Modular equation and equations • Prime and testing • Fermat's Theorem • Euler's Totient Function ø(n) • Zp • Groups • Rings • Finite Fields • Galois Field • Discrete Logarithms • Generator	▪ Watch the two pre-recorded videos before the class. ▪ Watch the class video on practice. ▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Optional math problem practice
5	Stream Cipher	• Stream Cipher • Linear Feedback Shift Registers • OFB and CFB • RC4 • Salsa20 • Chacha20	▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Do the class quiz
6	Block Cipher	• Block Cipher Design Principles • AES • 3DES	▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Do the class quiz

7	Modes of Operations	• Mode of operations • ECB • CBC • CTR • OFB • CFB • GCM*	▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Do the quiz ▪ Work on the team Project 3 due in 3 weeks
8	Public Key Scheme	• Public Key Scheme • Plain RSA Cryptosystem • Factoring and RSA Assumption • RSA-OAEP • ElGamal Encryption • Session Key • Digital signature • RSA FDH • RSA-PSS • ElGamal • DSA	▪ Watch the class video. ▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Do the quiz ▪ Work on the individual Project 4 due in 2 weeks
9	Cryptographic Hash Functions	• Types of collision resistance • Compression Function Construction • Merkle-Damgård Construction • Hash Family • SHA1 • SHA2 • SHA3 • Blockchain Hash Puzzle • More on operational modes (XTS, HCTR2, Accordion)	▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Do the class quiz
10	Mutual Authentication	• Message Authentication Codes • CMAC • HMAC • Authenticated Encryption • Digital Signature	▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Do the class quiz

11	Key Establishment and PKI	• Key Management • Key Distribution • Diffie Hellman Key Exchange • Key Encapsulation Mechanisms (KEM) • RSA KEM • DH KEM • Hybrid Encryption • Diffie-Hellman Integrated Encryption • The ElGamal public-key encryption • Certificates • Certificate Authorities • precertificate • CRL • Letsencrypt	▪ Watch the class video. ▪ Review with the slides. ▪ Read the references listed in the slides. ▪ Do the class quiz
12	PKI	• Certificates • Certificate Authorities • precertificate • CRL • Letsencrypt	▪ Watch the class recording. ▪ Review with the slides. ▪ Read the references listed in the Slide. ▪ Do the class quiz