Course Syllabus

Applied Cryptography

Instructor

Prof. Z Chen, PhD, CISSP
Use email: zxchen@ieee.org or wechat: zchenny for class communication.

Semester

Date: 9/2 – 11/23/2024
Zoom Sessions: T 8:20 – 11:35 AM (Beijing Time)
link: https://mercy.zoom.us/j/96893231634?pwd=2pZf62q9LjSOofXZptveneXRUrRe6w.1

Catalogues Description (new)

Introduction to the concepts and applications of cryptography and computer security. It covers basic building blocks of applied cryptography: block ciphers, stream ciphers, public-key encryption techniques, and mutual authentication such as cryptographic hash, message authentication codes and digital signatures, key establishment and KPI. The language of modern cryptography is primarily number theory, group theory and linear algebra, and various tools from them, including modular arithmetic, primality, fields and other algebraic structures are developed as needed. The course is aimed from the applied perspectives. Labs, class discussion and teamwork are emphasized throughout the course.
3 credits

Student Learning Outcome

After the class, students will be able to

(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 from Computer architecture and network are also helpful.

Course 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. (Aumasson) Serious Cryptography: A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson, 2017, online pdf
5. (EKR) A Pragmatic Introduction to Secure Multi-Party Computation, David Evans, Vladimir Kolesnikov, Mike Rosulek, 2022
6. https://securecomputation.org/docs/pragmaticmpc.pdf
7. https://www.coursera.org/learn/crypto.
8. online videos

Assessment

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

1. 10% Active Participation.
2. 40% Assignments.
3. 30% team projects
4. 20% one exam

Class Logistics

- Zoom Attendance is recorded. The link is given above.
- We will use the course management platform set by JianQiao and the TA, YU, Fan.
- WeChat class group will be set.
- Office hour: zoom session by appointment.
- Zoom and zoom etiquette
  - Use a computer, not a smart phone.
  - Find a quiet corner.
  - Show face or set up face photo in zoom settings plus official name.
  - Take notes and ask questions.
- Personal Computer with camera
  It is needed for the class projects and assignments. Mobile devices like smart phone or iPad are not for class and can be used only for emergency.

Success Tips

- A disciplined approach is a key to this class.
- Reading Habit
  Reading text line by line. Avoid scanning them too fast. Because contents need time digesting, students need to be patient and persistent. Taking notes and listing questions always.
- Internet search and AI assistant help
  Students may use the internet as their learning repository. Googling can be a starting point.
  It is ok in this class to use AI assistants. Students need to investigate them with a critical mind. Do not turn in its answers without further your curation and investigation.
- 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,

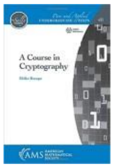
1. Do not to turn in the work of others
2. Do not give others the work to use as their own
3. Do not plagiarize from others (published or not)
4. Do not try to deceive the instructors

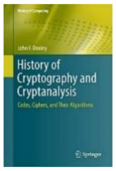
Remember, academic honesty does not prevent students from discussing any ideas and homework with their classmates and others. Such intellectual exchange is strongly encouraged.

Students W/ Disabilities

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

Bibliography

1.  ***A Course in Cryptography***, Heiko Knospe, American Mathematical Society, 2017, LCCN 2019011732 | ISBN 9781470450557

2.  *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

3. *A Graduate Course in Applied Cryptography, by* Dan Boneh and Victor Shoup, v0.5, Jan 2020, downloadable at http://toc.cryptobook.us/

4. *Cryptography and Network Security: Principles and Practice*, 7th edition, by William Stallings, 2017, Pearson, ISBN13: 978-0-13-444428-4

5. *Cryptography: An Introduction* by Smart, N. McGraw-Hill, 2002 (ISBN: 0077099877)

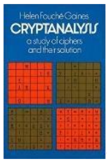
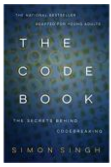
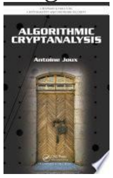
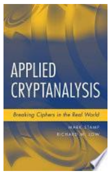
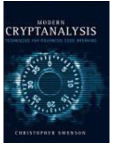
6. *Network Security, Private Communication in a Public World*, by Kaufman, Perlman, Speciner. 2nd Ed, Prentice-Hall. 2002 ISBN 0-13-046019-2.

7. *Hacking Exposed* by McClure, Scambray, Kurtz. 4th Ed, McGraw-Hill. 2003. ISBN 0072227427.

8. *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/

9. *A Graduate Course in Applied Cryptography* by D. Boneh & V. Shoup, downloadable at http://toc.cryptobook.us/

10. *Introduction to Modern Cryptography* (2nd edition) by J. Katz and Y. Lindell. CRC Press 2014 ISBN-13: 978-1466570269, check http://toc.cryptobook.us/

11. *Cryptanalysis, A Study of Ciphers and Their Solution*, by Helen F. Gaines, 1989
12. *The Code Book, The Secrets Behind Codebreaking*, by Simon Singh|, August 12, 2003
13. 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
14. Elementary Cryptanalysis, by Abraham Sinkov, Todd Feil, 2009
15. Heuristic Cryptanalysis of Classical and Modern Ciphers, by Ho Yean Li, 2015
16. Cryptanalysis of Number Theoretic Ciphers (Computational Mathematics) by Samuel S. Wagstaff Jr. 2003, Taylor and Francis, LLC
17.  Algorithmic Cryptanalysis, Antoine Joux, CRC Press, Jun 15, 2009
18.  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
19.  Modern Cryptanalysis: Techniques for Advanced Code Breaking, Christopher Swenson, John Wiley & Sons, Mar 17, 2008
20. https://en.wikipedia.org/wiki/Cryptanalysis
21. 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)

week	Module	contents	tasks
1	Crypto System Overview	• Good or bad guys • Crypto terminology • Cryptosystem or encryption Scheme • Security of a cryptosystem – definition • Security requirement – CIA and more • Breaking a cryptosystem - definition • Kerckhoff’s Principle • One time Pad • Stream ciphers, Block Ciphers, Public Key Scheme • Pseudo-random Functions and Permutations • One-Way Functions and Trapdoor One-Way Functions • Hash, Message Authentication Code , Digital Signature	Reading and catchup
2	Security Experiment Game	• Basic Security Notions and Security Notions w/ Oracles • Cryptographic Attack Models • Exhaustive Key Search • Ciphertext-only (Eavesdropping) attack • Known-plaintext attack • Chosen plaintext attack (CPA) • Chosen-ciphertext attack (CCA) • Chosen-key attack • Rubber-hose Attack • Pseudorandom Generators, Functions, permutations •	
3	Classical And Mechanical Encryption	• Simple Substitution • Poly-Alphabetic Substitution • Affine Cipher • Vigenere Cipher • Transposition Cipher • Scytale • Columnar Transposition • Statistical Analysis • Index of Coincidence • Enigma Machine ○ Rotors ○ Reflector ○ Stecker ○ Keys ○ Demo • Bombe known plaintext attacks	
4	Math Foundation	• Math Foundations • Modula Operations • Cyclic Group • Field • The extended Euclidean Algo	

		• Chinese Remainder Theorem • Prime • Discrete Logarithm	
5	Stream Cipher	• Stream Cipher • Linear Feedback Shift Registers • OFB and CFB • RC4 • Salsa20 • Chacha20 •	
6	Block Cipher	• Block Cipher Design Principles • AES • 3DES •	
7	Modes of Operations	• Mode of operations • ECB • CBC • CTR • OFB • CFB • GCM* (also in module MA) •	
8	Public Key Scheme	• Public Key Scheme • Plain RSA Cryptosystem • Factoring and RSA Assumption • RSA-OAEP • ElGamal Encryption • Session Key •	
9	Cryptographic Hash Functions	• Types of collision resistance • Compression Function Construction • Merkle-Damgård Construction • Hash Family • SHA1 • SHA2 • SHA3 • Blockchain Hash Puzzle •	
10	Mutual Authentication	• Message Authentication Codes • CMAC • HMAC • Authenticated Encryption • Digital signature • RSA FDH • RSA-PSS • ElGamal	

		• DSA	
11	Key Establishment	• 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	
12	PKI	• Certificates • Certificate Authorities • Pre-certificate • CRL • Letsencrypt	
13	One exam		