INF 521: Application of Cryptography to Information Security Problems
Fall 2017 Syllabus

Instructor	Email	Office	Office Hours	Lecture
Tatyana Ryutov	tryutov@usc.edu	TBD	Fridays 3:30pm–5:30pm	TeTh 11:00-12:50pm OHE 120

Course Website: https://piazza.com/usc/fall2017/inf521

Course Resources
Piazza will be used for lectures, announcements, assignments, and intra-class communication
DEN D2L will be used for:

- posting of grades
- homework submission
- quiz submission (DEN student only)

Office Hours
Fridays 3:30 p.m. – 5:30 p.m. Other hours are by appointment only. Students are advised to make appointments with the professor ahead of time and be specific with the subject matter to be discussed. Students should also be prepared for their appointment by bringing all applicable materials and information.

Grading
Grading method will be relative and on the curve.

Artifact	Weight	Date
Quizzes	20%	various
Midterm	25%	TBD
Final Exam	30%	December 12
HW Assignments	15%	various
Class Participation	10%	

Course Homework Submission
Homework submission in electronic form via DEN.

Late Policy
Cumulative of 10% times number of days late

- 1 day late: lose 10%
- 2 days late: lose 30% (10% + 20%)
- 3 days late: lose 60% (30% + 30%)

Greater than 4 days late not accepted.

No personal emergencies will be entertained (with the exception of the USC granted emergencies, in which case official documents need to be shown).

Required Textbooks:

CNS: "Cryptography and Network Security: Principles and Practice" (6th Edition) by William Stallings
HAC: "The Handbook of Applied Cryptography" by Menezes, van Oorschot, and Vanstone

Supplemental textbook:

Literature:

IdCrypto: C. Youngblood, "An Introduction to Identity-Based Cryptography," CSEP 590TU, 2005.

AnCom: Ren J and Wu J. Survey on Anonymous Communications in Computer Networks. Computer Communications. 2010, 33(4): 420–431.

TOR: R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium, August 2004.

Bitcoin: S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", http://www.bitcoin.org, 2008.

Zerocoin: Anonymous Distributed E-Cash from Bitcoin, Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin, IEEE Symposium on Security and Privacy (Oakland) 2013.

PUF: Ruhrmair, U., and Holcomb, D. E. PUFs at a glance. In Proceedings of the conference on Design, Automation & Test in Europe (2014), European Design and Automation Association, p. 347.

Quantum: European Telecommunications Standards Institute White Paper No. 8, Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, June 2015.

Course Objectives
At the end of the course, the students will achieve the following:

- A strong grasp of the basic concepts underlying classical and modern cryptography, and the fundamentals.
- Understand how security is defined and proven at the cryptographic level.
- Understand common attacks and how to prevent them.
- Gain the ability to apply appropriate cryptographic techniques to a security engineering (and management) problem at hand.

Course Structure
The first part of the course will cover the concepts and theory of cryptography. The second part of the course will focus on applications of cryptography in various security domains.

Methods of Teaching
The primary teaching method will be lectures, discussion, and case studies. The students are expected to take an active role in the course. Students will attend lectures and actively participate in the classroom. They will complete homework and exams to reinforce the concepts taught.

There will be several quizzes, homework/laboratory assignments. No programming will be necessary for this course.

Course Homework Submission
Homework submission in electronic form via DEN.

Projected Schedule
Class sequence, dates, reading assignments, and topics are subject to change as the semester proceeds. Any revisions will be noted and announced in class and posted on the class website.

Week	Tu/Th	Topic	Reading
1	8/22 8/24	1. Introduction, crypto history 2. Attacks on crypto, one time pad, perfect secrecy	HAC: 1.2, 1.4 HAC: 1.13; CNS: 1.3,1.4
2	8/29 8/31	3. Stream ciphers, semantic security 4. Block ciphers, DES	HAC: 1.5; CNS: 2.1,2.2 CNS: 3.1, 3.2; 6.1
3	9/5 9/7	5. Attacks on block ciphers, AES 6. Using block ciphers, EBC	CNS: 3.4, 5.2 CNS: 6.2
4	9/12 9/14	7. Using block ciphers, CBC, CTR 8. Message integrity, MAC	CNS: 6.3, 6.6 CNS: 12.1-12.4
5	9/19 9/22	9. Collision resistance 10. Authenticated encryption	HAC: 9.2 CNS: 2.7
6	9/26 9/28	11. Deterministic encryption 12. Basic key exchange	
7	10/3 10/5	13. Number theory review, public key crypto intro 14. Public key crypto: RSA	CNS: 4.1-4.5 CNS: 9.1, 9.2

8	10/10 10/12	15.Public key crypto: El Gamal, midterm review **Midterm (tentatively)**	CNS: 10.2
9	10/17 10/19	16. Digital signatures 17. Key management and distribution, digital certificates	CNS: 13.1-13.5 CNS: 14.1-14.3
10	10/24 10/26	18. PKI, identity based encryption 19. Identification and authentication, zero knowledge protocols, Kerberos	CNS: 14.4,14.5; IdCrypto CNS: 15.1-15.4
11	10/31 11/2	20. Electronic mail security, PGP 21. Web and transport level security, SSH, TLS/SSL	CNS: 19.1 CNS: 17
12	11/7 11/9	22. IP security, wireless network security 23. Anonymous communication, Tor	CNS: 18, 20.1, 20.2 AnCom, TOR
13	11/14 11/16	24. Cryptocurrencies, Bitcoin 25. Hardware–based security, side channel attacks	Bitcoin, Zerocoin
14	11/21 11/23 11/25	26. Physically Unclonable Function, Trusted Platform Module **NO class - Thanksgivings**	PUF
15	11/28 11/30	27. Quantum safe cryptography, Cloud security 28. Final exam review	Quantum; CNS: 16.4,16.5

Academic Conduct

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in SCampus in Section 11, Behavior Violating University Standards https://scampus.usc.edu/1100-behavior-violating-university-standards-and-appropriate-sanctions. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Discrimination, sexual assault, and harassment are not tolerated by the university. You are encouraged to report any incidents to the Office of Equity and Diversity http://equity.usc.edu or to the Department of Public Safety http://adminopsnet.usc.edu/department/department-public-safety. This is important for the safety of the whole USC community. Another member of the university community – such as a friend, classmate, advisor, or faculty member – can help initiate the report, or can initiate the report on behalf of another person. The Center for Women and Men http://www.usc.edu/student-affairs/cwm/ provides 24/7 confidential support, and the sexual assault resource center webpage http://sarc.usc.edu describes reporting options and other resources.

Support Systems

A number of USC's schools provide support for students who need help with scholarly writing. Check with your advisor or program staff to find out more. Students whose primary language is not English should check with the American Language Institute

http://dornsife.usc.edu/ali, which sponsors courses and workshops specifically for international graduate students. The Office of Disability Services and Programs http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html provides certification for students with disabilities and helps arrange the relevant accommodations. If an officially declared emergency makes travel to campus infeasible, USC Emergency Information http://emergency.usc.edu will provide safety and other updates, including ways in which instruction will be continued by means of blackboard, teleconferencing, and other technology.

Students with Disabilities

Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me as early in the semester as possible. Your letter must be specific as to the nature of any accommodations granted. DSP is located in STU 301 and is open 8:30 am to 5:30 pm, Monday through Friday. The telephone number for DSP is (213) 740-0776.