# CSCI531: Applied Cryptography
## Spring 2021 Syllabus

| Instructor | Email | Office Hours | Lecture |
|---|---|---|---|
| Tatyana Ryutov | tryutov@usc.edu | TBD via Zoom | Wednesday 2:00-5:20pm, via Zoom/Webex |

**Course Resources**
Piazza https://piazza.com/usc/spring2021/csci531 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)

**Grading**

| Artifact | Weight |
|---|---|
| Quizzes | 15% |
| Midterm | 20% |
| Final Exam | 20% |
| HW Assignments | 10% |
| Programming Assignments | 10% |
| Semester Project | 15% |
| Class Participation | 10% |

**Course Homework Submission**
Homework submission in electronic form via DEN D2L.

**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 Textbooks:**

"Introduction to modern cryptography" Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008.

"A Graduate Course in Applied Cryptography" Dan Boneh and Victor Shoup, 2020, http://toc.cryptobook.us/

**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, two programming assignments, and semester project.

**Course Homework Submission**

Homework submission in electronic form via DEN D2L.

**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.

| Lectures | Topics | Readings |
|---|---|---|
| **Lecture 1** 1/20 | Introduction, Attacks on crypto, Crypto history, One time pad | HAC: 1.2, 1.4<br>HAC: 1.13; CNS: 1.3,1.4 |
| **Lecture 2** 1/27 | Perfect secrecy, Stream ciphers, Semantic security | HAC: 1.5; CNS: 2.1,2.2<br>CNS: 3.1, 3.2; 6.1 |
| **Lecture 3** 2/3 | Block ciphers, DES, Attacks on block ciphers, AES | CNS: 3.4, 5.2<br>CNS: 6.2<br>**Quiz 1** |
| **Lecture 4** 2/10 | Using block ciphers, EBC, CBC, CTR | CNS: 6.3, 6.6<br>CNS: 12.1-12.4 |
| **Lecture 5** 2/17 | Message integrity, MAC, Collision resistance | HAC: 9.2<br>CNS: 2.7 |
| **Lecture 6** 2/24 | Authenticated encryption | CNS: 4.1-4.5<br>**Quiz 2** |
| **Lecture 7** | Basic key exchange, Number theory review, Public | CNS: 9.1, 9.2 |

| | | |
|---|---|---|
| 3/3 | key crypto intro, RSA, El Gamal | CNS: 10.2 |
| **Lecture 8**<br>3/10 | Key management and distribution, Digital signatures, Digital certificates, PKI, Identity based encryption | CNS: 13.1-13.5<br>CNS: 14.1-14.3<br>CNS: 14.4,14.5<br>IdCrypto |
| 3/17 | **Midterm**<br>**Topic TBD** | |
| **Lecture 9**<br>3/24 | Identification and authentication, Zero knowledge protocols, Kerberos, Electronic mail security | CNS: 15.1-15.4<br>CNS: 19.1<br>**Quiz 3** |
| **Lecture 10**<br>3/31 | Web and transport level security,<br>IP security, Wireless network security | CNS: 17<br>CNS: 18, 20.1, 20.2 |
| **4/7** | **No lecture, University Wellness day** | |
| **Lecture 11**<br>4/14 | Anonymous communication, TOR,<br>Cryptocurrencies, Bitcoin | AnCom, TOR |
| **Lecture 12**<br>4/21 | Hardware–based security, Physically Unclonable Function, Trusted Platform Module | PUF<br>**Quiz 4** |
| **Lecture 13**<br>4/28 | Quantum cryptography,<br>Course review | Quantum |
| **Final Exam** | **May 10, 2-4 p.m.** | |

## Synchronous session recording notice

Live class sessions will be recorded and made available to students through Blackboard (including transcriptions). Please remember that USC policy prohibits sharing of any synchronous and asynchronous course content outside of the learning environment. As a student, you are responsible for the appropriate use and handling of these recordings under existing SCampus policies regarding class notes (https://policy.usc.edu/scampus-part-c/). These rules will be strictly enforced, and violations will be met with the appropriate disciplinary sanction.

## Going back to Campus

Although we are starting the semester with online instruction only, conditions may improve**.** In such case, courses listed as hybrid will give opportunity to students to attend class in person. This will happen only by following the strictest health guidelines and safety protocols. These are listed in the Trojans Return page. Please take the time to read this ahead so that you are prepared in case it is possible to return to in-person instruction.

## Learning Experience Evaluations

Learning Experience Evaluations will be completed during the last day of class. This will be your opportunity to provide feedback about your learning experience in the class. This feedback helps the instructor determine whether students are having the intended learning experiences for the class. It is important to remember that the learning process is collaborative and requires significant effort from the instructor, individual students, and the class as a whole. Students should provide a thoughtful assessment of their experience, as well as of their own effort, with comments focused on specific aspects of instruction or the course. Comments on personal characteristics of the instructor are not appropriate and will not be considered. For this feedback to be as comprehensive as possible, all students should complete the evaluation.

## 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 Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on scientific misconduct, policy.usc.edu/scientific-misconduct.

## 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.

## Support Systems

*Counseling and Mental Health - (213) 740-9355 – 24/7 on call*
studenthealth.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

*National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call*
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

*Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL), press "0" after hours – 24/7 on call*
studenthealth.usc.edu/sexual-assault
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

*Office of Equity and Diversity (OED) - (213) 740-5086 | Title IX – (213) 821-8298*
equity.usc.edu, titleix.usc.edu
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

*Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298*
usc-advocate.symplicity.com/care_report
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office of Equity and Diversity |Title IX for appropriate investigation, supportive measures, and response.

*The Office of Disability Services and Programs - (213) 740-0776*
dsp.usc.edu

Support and accommodations for students with disabilities. Services include assistance in providing readers/notetakers/interpreters, special accommodations for test taking needs, assistance with architectural barriers, assistive technology, and support for individual needs.

*USC Campus Support and Intervention - (213) 821-4710*
campussupport.usc.edu
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

*Diversity at USC - (213) 740-2101*
diversity.usc.edu
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

*USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call*
dps.usc.edu, emergency.usc.edu
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

*USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call*
dps.usc.edu
Non-emergency assistance or information.

*Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)*
ombuds.usc.edu
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.