**CS 486-01:**

Course Meeting Time(s) / Seat Time

Class 11:45 am – 1:30 pm MW

Lo Schiavo G12 Aug 23, 2017 - Dec 13, 2017

Number of Units 4

Instructor: Paul A. Lambert Office Hours: 2:00-3:00 MW

Office: 403A or by appointment

Email: plambert@usfca.edu

Phone: +1-650-787-9141

**Prerequisites:**

Data Structures (CS 245) is a pre-requisite.

**Texts and Materials:**

Material will be provided as the course progresses. Reading and references include:

* **TABC:** (free)  *[The American Black Chamber](http://marshallfoundation.org/library/wp-content/uploads/sites/16/2014/09/WFFvol05watermark.pdf)* by Herbert O. Yardley (as annotated by William F. Friedman).
* **MoC:** (free) [Manual of Cryptography](http://marshallfoundation.org/library/wp-content/uploads/sites/16/2014/09/WFFvol05watermark.pdf), the War Office.
* **Boneh-Shoup:** (free) [*A Graduate Course in Applied Cryptography*](http://toc.cryptobook.us) by D. Boneh and V. Shoup
* **HAC:** (free)  *[Handbook of Applied Cryptography](http://www.cacr.math.uwaterloo.ca/hac/)* by A. Menezes, P. Van Oorschot, S. Vanstone.
* **TCB:** [*The Code Book*](https://simonsingh.net/cryptography/), by Simon Singh.
* **PMC**: (free) [*A Mathematical Theory of Cryptography*](https://www.iacr.org/museum/shannon45.html), by Claude Shannon.
* <https://theintercept.com/snowden-sidtoday/>
* **TCM**: [The Cypherpunk Manifesto](https://www.activism.net/cypherpunk/manifesto.html)

**Course Overview:**

Cryptography historically has been the study of techniques for secret communications. Contemporary cryptography looks more broadly at the ways to protect the information and is a fundamental building block of electronic commerce and our expanding virtual communities. This course will cover the history and fundamentals of modern cryptography. Contemporary applications of cryptography will be examined in detail including the legal and political implications of the technology. Programming assignments will produce a toolkit of useful cryptographic tools and will cumulate in individual projects.

The course material will include: classic cryptography, cryptanalysis, steganography, modern mathematical cryptography, post-quantum cryptography, cryptographic protocols, and the legal and social ramifications of cryptography. Students will be expected to display knowledge of both theory and practice through written examinations and programming assignments.

**Instructor Specific Policies:**

Grades will be based on class participation (10%), homework assignments (30%), projects (30%) and a final exam (20%).

**Preliminary Schedule:**

August W-23: First Class, Introductions, Overview

August M-28:History and classic cryptography, *Last day to add classes*

August W-30: HW1 and HW2 due.

September M-4: No class, Labor Day

September W-6: HW3 due.

*Friday September 8—Census Date (last day to drop classes with a refund)*

October M-16: No class, Fall Break

*November 3–* *Last day to drop classes or withdraw*

December M-4: Project Presentations

December W-6: Project Presentations, Last day of class

December W-13 (10:00 am – 12:00 pm): **Final Exam**, location TBD

**Course Learning Outcomes:**

Students will learn to apply cryptographic techniques and have a strong understanding of cryptographic theory necessary to evaluate cryptographic designs.

**Academic Integrity:**

As a Jesuit institution committed to cura personalis—the care and education of the whole person—USF has an obligation to embody and foster the values of honesty and integrity. USF upholds the standards of honesty and integrity from all members of the academic community. All students are expected to know and adhere to the University's Honor Code. You can find the full text of the code online at <http://myusf.usfca.edu/academic-integrity/>. The policy covers:

* Plagiarism — intentionally or unintentionally representing the words or ideas of another person as your own; failure to properly cite references; manufacturing references.
* Working with another person when independent work is required.
* Submission of the same paper in more than one course without the specific permission of each instructor.
* Submitting a paper written by another person or obtained from the internet.
* The penalties for violation of the policy may include a failing grade on the assignment, a failing grade in the course, and/or a referral to the Academic Integrity Committee.

**Students with Disabilities:**

If you are a student with a disability or disabling condition, or if you think you may have a disability, please contact USF Student Disability Services (SDS) at [415 422-2613](tel:415%20422-2613) within the first week of class, or immediately upon onset of disability, to speak with a disability specialist.

If you are determined eligible for reasonable accommodations, please meet with your disability specialist so they can arrange to have your accommodation letter sent to me, and we will discuss your needs for this course. For more information, please visit: <http://www.usfca.edu/sds> or call [(415) 422-2613](tel:%28415%29%20422-2613).

**Behavioral Expectations:**

All students are expected to behave in accordance with the Student Conduct Code and other University policies (see <http://www.usfca.edu/fogcutter/>). Open discussion and disagreement is encouraged when done respectfully and in the spirit of academic discourse. There are also a variety of behaviors that, while not against a specific University policy, may create disruption in this course. Students whose behavior is disruptive or who fail to comply with the instructor may be dismissed from the class for the remainder of the class period and may need to meet with the instructor or Dean prior to returning to the next class period. If necessary, referrals may also be made to the Student Conduct process for violations of the Student Conduct Code.

**Learning, Writing, and Speaking Centers:**

The Learning, Writing, and Speaking Centers at USF provide individualized support to assist you in better understanding course material and to aid you on your path to success. Services are free and include one-on-one tutoring, group tutoring, and one-on-one Academic Skills Coaching appointments to discuss effective study strategies. The Learning Center supports over 80 courses each semester. The Writing Center helps students develop their writing skills in rhetoric, organization, style, and structure, through one-on-one interactive conferences. The Speaking Center helps students prepare for public speaking — including speeches, oral presentations, team presentations, and visual aid demonstrations. International students may also contact us to learn more about communicating with professors and general academic study skills. The Learning, Writing, and Speaking Centers are located on the Lower Level of Gleeson Library. Please contact them at 415-422-6713 for further assistance or visit <https://myusf.usfca.edu/student-life/lwc> to make an appointment.

**Counseling and Psychological Services:**

Our diverse staff offers brief individual, couple, and group counseling to student members of our community. CAPS services are confidential and free of charge. Call [415-422-6352](tel:415-422-6352) for an initial consultation appointment. Having a crisis at 3 AM? We are still here for you. Telephone consultation through CAPS After Hours is available between the hours of 5:00 PM to 8:30 AM; call the above number and press 2.

**Confidentiality, Mandatory Reporting, and Sexual Assault:**

As an instructor, one of my responsibilities is to help create a safe learning environment on our campus. I also have a mandatory reporting responsibility related to my role as a faculty member. I am required to share information regarding sexual misconduct or information about a crime that may have occurred on USFs campus with the University. Here are other resources:

• To report any sexual misconduct, students may visit the Title IX Coordinator

Leighia Fleming (UC 5th floor) or see many other options by visiting our website:

[https://myusf.usfca.edu/title-ix](https://myusf.usfca.edu/title-ix" \t "_blank)

• Students may speak to someone confidentially, or report a sexual assault confidentially by contacting Counseling and Psychological Services at 415-422-6352 or speaking to a clergy member in University Ministry at 415-422-4463.

**•** To find out more about reporting a sexual assault and resources at USF, visit USFs Callisto website at: [https://usfca.callistocampus.org/](https://usfca.callistocampus.org/" \t "_blank).

**•** For an off-campus resource, contact San Francisco Women Against Rape (SFWAR) [(415) 647-7273](tel:%28415%29%20647-7273" \t "_blank) ([www.sfwar.org](http://www.sfwar.org" \t "_blank)).

**Student Accounts - Last day to withdraw with tuition reversal:**

Students who wish to have the tuition charges reversed on their student account should withdraw from the course(s) by the end of the business day on the last day to withdraw with tuition credit (census date) for the applicable course(s) in which the student is enrolled. Please note that the last day to withdraw with tuition credit may vary by course. The last day to withdraw with tuition credit (census date) listed in the Academic Calendar is applicable only to courses which meet for the standard 15-week semester. To find what the last day to withdraw with tuition credit is for a specific course, please visit the Online Class Schedule at [www.usfca.edu/schedules](http://www.usfca.edu/schedules).

**Financial Aid - FAFSA priority filing deadline (undergraduates only):**

March 2 - Priority filing deadline for FAFSA (The Free Application for Federal Student Aid - <https://fafsa.ed.gov/>) for continuing undergraduates.