



WASTC 2018 Faculty Development Weeks

Cryptography and Blockchains

Dates: In Person, June 11 - 15, 2018 Cabrillo College, Aptos CA

Individuals, companies, and governments all have private data on their computer systems that must be protected. However, the encryption techniques required to protect them are difficult to apply, and often fail in practice. There is a serious shortage of information technology professionals who are qualified to install, repair, and maintain cryptographic security measures. This class helps students prepare to meet those needs.

Mathematical underpinnings and practical applications of modern cryptographic systems, including the Advanced Encryption Standard (AES), the Secure Hash Algorithms (SHA), and Rivest-Shamir-Adleman (RSA). The class focuses on practical applications: selecting, implementing, testing, and maintaining systems to protect data on modern computer networks.

By the end of the course, students will be prepared to:

- Implement modern cryptographic systems, including AES, RSA, and SHA
- Choose appropriate methods to protect data at rest, in use, and in motion
- Perform attacks to reveal encrypted data
- Explain the strengths and weaknesses of modern cryptographic systems
- Compare and evaluate blockchain and cryptocurrency systems including Bitcoin, Ethereum, and Multichain

Prerequisites: Familiarity with security concepts at the Security+ level, and familiarity with algebra.

Recommended Textbooks:

Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar, Jan Pelzl, and Bart Preneel, ISBN: 3642041000 ASIN: B014P9I39Q

Mastering Bitcoin: Unlocking Digital Cryptocurrencies 1st Edition by Andreas M. Antonopoulos, ISBN: 1449374042 (optional, free online)

Instructor: Sam Bowne, Ph.D.



Sam Bowne has been teaching computer networking and security classes at CCSF since 2000. He has given talks and hands-on trainings at DEFCON, HOPE, B-Sides SF, B-Sides LV, BayThreat, LayerOne, Toorcon, and many other schools and conferences.

Degrees: B.S. in Physics from Edinboro University of Pennsylvania and a Ph.D. in Physics from University of Illinois, Urbana-Champaign.
Certificates: Current CISSP; older certificates from Cisco, Juniper, Microsoft, and others..

Sponsored by:



WESTERN ACADEMY
SUPPORT & TRAINING CENTER