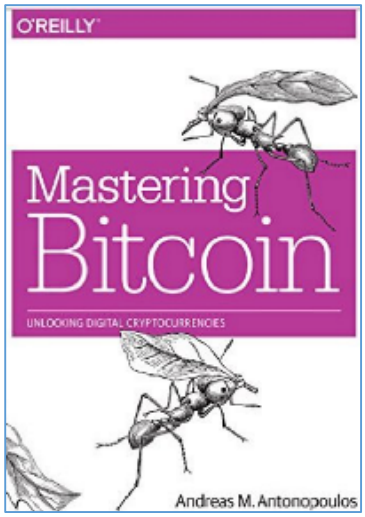
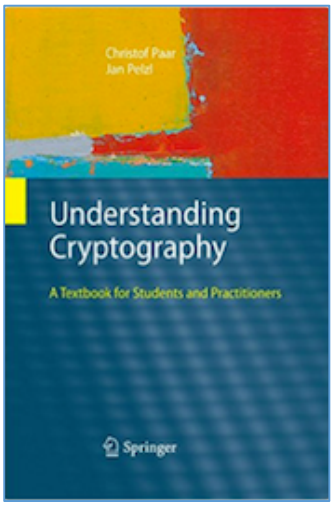


Optional, free

CNIT 141: Cryptography for Computer Networks

Fall 2017 Sam Bowne

77820 M 6:10-09:00PM
SCIE 200



Required
$22 from Amazon

Course Justification

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.

Catalog Description

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.

Prerequisites: CNIT 120 or equivalent familiarity with the fundamentals of security, and MATH 40 or equivalent familiarity with algebra

Student Learning Outcomes

Upon successful completion of this course, the student will be able to:

A. **Implement modern cryptographic systems, including AES, RSA, and SHA**
B. **Choose appropriate methods to protect data at rest, in use, and in motion**
C. **Perform attacks to reveal encrypted data**
D. **Explain the strengths and weaknesses of modern cryptographic systems**

Textbooks

Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar, Jan Pelzl, and Bart Preneel, ISBN: 3642041000 ASIN: B014P9I39Q Buy from Amazon ($22)

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

Live Streaming

You can attend class remotely using Zoom. A conference will start each Monday at 6 pm.

Join from PC, Mac, Linux, iOS or Android: https://zoom.us/j/128470103

Or iPhone one-tap (US Toll): +16465687788,,128470103# or +14157629988,,128470103#

Or Telephone: Dial: +1 646 568 7788 (US Toll) or +1 415 762 9988 (US Toll) Meeting ID: 128 470 103 International numbers available: https://zoom.us/zoomconference?m=Sd3zjINfTg5mo4nTtFIlzSWHpKACTSLh

The free version of Zoom is limited to 40 minutes per meeting. So to see the second part of the lecture live, you may have to join with this meeting ID: 387-892-4534 or this link:

https://zoom.us/j/3878924534

Classes will also be recorded and published on YouTube for later viewing.

Schedule (may be changed)

Date	Quiz & Proj Due	Topic
Mon 8-21		**Intro: Bitcoin & Cryptography**
Mon 8-28		**1. Introduction to Cryptography and Data Security**
Mon 9-4	***Holiday - No Class***	
Fri 9-8	***Last Day to Add Classes***	
Mon 9-11	**Quiz Ch 1-2 * Proj 1 & 2 due**	**2. Stream Ciphers**
Mon 9-18	**Quiz Ch 3 * Proj 3 due**	**3. The Data Encryption Standard (DES) and Alternatives**
Mon 9-25	**Quiz Ch 4 * Proj 4 & 5 due**	**4. The Advanced Encryption Standard (AES)**
Mon 10-2	**Quiz Ch 5 * Proj 6 due**	**5. More About Block Ciphers**
Mon 10-9	***Holiday - No Class***	
Mon 10-16	**Quiz Ch 6 * Proj 7 & 8 due**	**6. Introduction to Public-Key Cryptography**
Mon 10-23	**Quiz Ch 7 * Proj 9 due**	**7. The RSA Cryptosystem**
Mon 10-30	**Quiz Ch 8 * Proj 10 & 11 due**	**8. Public-Key Cryptosystems Based on the Discrete Logarithm Problem**
Mon 11-6	**Quiz Ch 9 * Proj 12 Due**	**9. Elliptic Curve Cryptosystems**
Mon 11-13	**No Quiz No Proj due**	**Guest Speaker: TBA (may be rescheduled)**
Mon 11-20	**Quiz Ch 10 * Proj 13 & 14 due**	**10. Digital Signatures**
Mon 11-27	**Quiz Ch 11 * Proj 15 due**	**11. Hash Functions**
Mon 12-4	**Quiz Ch 12 * Proj 16 & 17 due**	**12. Message Authentication Codes (MACs)**
Mon 12-11	**Quiz Ch 13 * All Extra Credit Proj due**	**Last Class: 13. Key Establishment**
Mon 12-18	**Final Exam**	

**** Quizzes due 30 min. before class***