NYU COURANT INSTITUTE OF MATHEMATICAL SCIENCES

Applied Cryptography & Network Security

NYU | COURANT COMPUTER SCIENCE

- **Course: CSCI-GA.3205 Applied Cryptography & Network Security**
- **Instructor: Dr. Mazdak Zamani**
- **Email Address: mazdak.zamani@NYU.edu**

Course Description:

This course provides a comprehensive overview of network security. It covers authentication methods along with common network attacks and how to safeguard against the network devices and media, and the proper use of perimeter topologies such as DMZs, Extranets, and Intranets to establish network security. Operational/Organizational sec Disaster Recovery, and Business Continuity, as well as coverage of Computer Forensics and how it relates to further avenues of specialization for the security student. Crypt differences between asymmetric and symmetric algorithms, and the different types of PKI certificates and their usage. Students also learn the core cryptographic tools, inclu digital signature, key agreement protocols, etc., are used behind millions of daily on-line transactions.

Course Objectives:

At the end of the course the student will be able to:

- Identify risks, threats and challenges that information systems/network face.
- Demonstrate operating knowledge of information security fundamentals.
- Identify and be able to select and purchase elements of network infrastructure.
- Recommend tests of the defenses of an organization network structure.
- Demonstrate ability to manage and protect advanced communications.
- Understand basic principles of cryptography and general cryptanalysis.
- Be acquainted with the concepts of symmetric encryption and authentication.
- Know and understand public key encryption, digital signatures, and key establishment.
- Be able to compose, build and analyze simple cryptographic solutions.
- Know and understand common examples and uses of cryptographic schemes, including the AES, the Digital Signature Algorithm, and the basic Diffie-Hellman key estal apply them.

Teaching-Learning Strategies:

An important component of the course is the ability to frequently access Brightspace to view lecture slides, quizzes, and assignments. All assignments are to be submitted el have access to a good computer facility with Internet access, plus productivity software such as Microsoft Office.

Textbooks & Materials:

- Introduction to Modern Cryptography, J. Katz and Y. Lindell. Chapman and Hall/CRC;. ISBN-13: 978-1466570269. 2014.
- A Graduate Course in Applied Cryptography. Dan Boneh and Victor Shoup.2020.
- Introduction to Cryptography with Coding Theory, 2nd Edition. Trappe, 2006. ISBN-13: 9780131743625.
- CompTIA Security+ Guide to Network Security Fundamentals, 5th Edition (Cengage Learning), ISBN: 978-1-305-09394-2.2015.

Grading/Evaluation Methods

	Number of Assignments	Points per Submission	Total Points
Assignment/ Projects	11	10	110
Quiz/ Research	11	10	110
Attendance/ Participation/ Discussion	15	3	45
Final Research Report and Presentation	1	75	75
Midterm Exam	1	80	80
Final Exam	1	80	80
Total			500

Course Content:

Dates	Topic(s)	Reading	Assignment /Projects	Quiz/ Research	Attendance/ Participation/ Discussion
Unit 1:	• Symmetric vs Asymmetric Cryptography • Kerckhoffs' principle • Statistical patterns • Substitution (Shift & Vigenère Cipher) • Principles of Modern Cryptography • Threat models	Chapter 1 (Katz-2014)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 2:	• Perfectly Secret Encryption • One-Time Pad (Vernam Cipher) • Limitations of Perfect Secrecy • Shennon's Theory • Computational Ciphers • Semantic Security	Chapter 2 (Katz-2014)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 3:	• Stream Ciphers • Block Cipher (DES, AES)	Chapter 2 & 3 & 4 (Boneh-2020)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 4:	• Message Integrity • Message Authentication Code • Collision resistant hashing • Authenticated Encryption	Chapter 6 & 7 & 8 & 9 (Boneh-2020)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 5:	• Public key tools • Trapdoor permutation scheme - RSA • Key exchange based on the RSA • Diffie-Hellman key exchange • Merkle puzzles	Chapter 10 (Boneh-2020)	10 points - Due by next week	10 points - Due by next week	3 points

Dates	Topic(s)	Reading	Assignment /Projects	Quiz/ Research	Attendance/ Participation/ Discussion
Unit 6:	• Public key encryption • ElGamal encryption • Digital Signature	Chapter 11 & 13 (Boneh-2020)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 7:	• Affine Cipher • Attacks Review • Steganography	Chapter 2 (Trappe-2006)	10 points - Due by next week	10 points - Due by next week	3 points
Midterm:	Midterm Exam		80 points		
Unit 8:	• Introduction to Security • Threats • Malware and Social Engineering Attacks • Application and Networking- Based Attacks	Chapter 1 & 2 & 3 (CompTIA Security+)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 9:	• Application, Data, and Host Security • Securing Network Devices • Network Security Hardware • Securing the operating system (OS) • Pretty Good Privacy (PGP) • Security Through Network Design Elements	Chapter 4 & 7 (CompTIA Security+)	10 points - Due by next week	10 points - Due by next week	3 points

Dates	Topic(s)	Reading	Assignment /Projects	Quiz/ Research	Attendance/ Participation/ Discussion
Unit 10:	Administering a Secure Network • TCP/IP Protocols • Monitoring and analyzing logs • Port security • HTTPS, SSH, TLS/SSL	Chapter 8 (CompTIA Security+) Sections 9.8 & 9.9 (Boneh-2020)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 11:	Wireless Network Security • Wireless Attacks • Wireless Security Solutions ○ Wired Equivalent Privacy (WEP) ○ Wi-Fi Protected Access (WPA) ○ IPsec	Chapter 9 (CompTIA Security+) Sections 9.10 & 9.11 (Boneh-2020)	10 points - Due by next week	10 points - Due by next week	3 points
Unit 12:	Research Report and Presentation		75		3 points
Unit 13:	Research Report and Presentation				3 points
Final Exam:	Final Exam		80 points		

Dr. Mazdak Zamani

Adjunct Assistant Professor
Courant Institute of Mathematical Sciences
New York University
Graduate Division
Computer Science
251 Mercer, New York, NY 10012
Warren Weaver Hall, Office 308
Email Address: mazdak.zamani@NYU.edu
Phone: (212) 998-3078
Ext: 8-3078
Google Scholar page

Applied Cryptography & Network Security