

Encryption Methods and Techniques CSSS-5160

S2 2021 Section HH 3 Credits 03/15/2021 to 05/14/2021 Modified 03/03/2021

Meeting Times

Lecture

Tuesday, 6:00 PM to 10:00 PM, CSSS 5160- Via Zoom out of Henderson Hall With sections W1 & GO

Please realize that all times will be at 1800 ET time - regardless of how Webster stores and reports times. We will always start class at 1800 (6:00 pm) ET/5:00 CT/4:00 MT/3:00 PT

For the Zoom link please login to WorldClassroom on the left side there is a zoom link - click on that. All meeting links posted in there.

Contact Information

Instructor: Don George MS

Email: donaldgeorge34@webster.edu

Phone: (703) 909-2740

NOTE: The University is requiring to teach out of all three books and therefore all be required. However, we will focus on only two of them:

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

Author: Simon Singh

Publisher: Anchor; Reprint edition (2000)

ISBN-10: 0385495353

ISBN-13: 978-0385495325

-- AND --

Understanding Cryptography: A Textbook for Students and Practitioners

Authors: Christof Paar and Jan Pelzi

Publisher: Springer; 1st edition (2010)

ISBN-10: 3642041000

ISBN-13: 978-3642041006

Description

The history and application of ciphers, codes and encryption/ decryption methods and techniques are examined in detail. Public and Private keys and other advanced methods will be included. Understanding the overhead of encryption on communications systems and the storage of data as well as methods employed for decryption, verification and authentication. Aspects of ethics and information privacy have a role when security is applied to public systems and email content as well as higher levels of security for corporations proprietary and government classified information; additionally, the Data Protection Act will be discussed.

Outcomes

The student will:

- Summarize and demonstrate an understanding of the vocabulary of cybersecurity terms and phraseology.
- Acquire and differentiate a broad understanding of the cybersecurity strategic operations environment, including methods, ethics, laws, policies and procedures.
- Demonstrate and differentiate a basic working knowledge of Encryption/Decryption methods including Private-Key, Public-Key, Pseudorandomness, Encryption and Digital Signature Schemes, Algorithmic Number Theory, as well as system vulnerabilities, and growing threats.

- Describe the roles, responsibilities, and tools of a cybersecurity encryption technician or security program manager.
- Explain their basic knowledge of critical cybersecurity infrastructures, communications, encryption detection and protection schemes, and potential threats and impacts.
- Summarize and discuss an understanding of the basics of the Comprehensive National Cybersecurity Initiative (CNCI) and the National Security Space Strategy, and the Department of Defense Space Policy Directive.
- Differentiate the scope of the evolving environment of cybersecurity communications as well as international space laws and policies.
- Classify future trends in cybersecurity strategic space operation issues facing commercial and national assets.
- Produce graduate level research papers and practice oral presentation methods.
- Demonstrate their understanding and proper application of APA as it is applied to professional writing.
- Demonstrate skills in the use of common graduate program technologies – PowerPoint, Internet Research (Wikipedia is not considered a valid source), Library Resources, e-Reserves, Concourse, Connections and Turnitin.
- Categorize the challenges of the Cybersecurity (MS) program and the importance of thinking about the capstone course in terms of their research focus or projects.
- Synthesize and integrate the learning experiences acquired throughout the MS in Cybersecurity program, apply critical thinking and evaluation methods of current and future topics relative to this major.

Required Textbook

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

Author: Singh

Publisher: Anchor

Edition: 2000

ISBN: 978-0385495325

Materials

Required Textbooks: *(see notes in CONTACT heading)*

Applied Cryptography: Protocols, Algorithms, and Source Code in C

Author: Bruce Schneier

Publisher: Wiley; 2nd Edition (1995)

ISBN-10: 0471117099

ISBN-13: 978-0471117094

-- AND --

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

Author: Simon Singh

Publisher: Anchor; Reprint edition (2000)

ISBN-10: 0385495353

ISBN-13: 978-0385495325

-- AND --

Understanding Cryptography: A Textbook for Students and Practitioners

Authors: Christof Paar and Jan Pelzi

Publisher: Springer; 1st edition (2010)

ISBN-10: 3642041000

ISBN-13: 978-3642041006

Textbook title and ISBN posted here:

<http://www.bkstr.com/websteronlinestore/home>

Start here - follow drop down menus

Deliverables

Please see the Evaluation section for the course deliverables.

Evaluation

Criteria

- 10% - Class Participation
- 20% - Term Paper on Week 8 on encryption methods used in Federal agencies
- 30% - Midterm usually held on Week 5
- 40% - Cumulative Final on Week 9

Schedule

When	Topic	Notes
Lecture Week 1	Combined Readings	Understanding Cryptography: Chapter 1 - Introduction to Cryptography and Data Security The Code Book - Chapter 1 - The Cipher of Mary Queen of Scots Homework to assigned <u>in class</u> from questions at end of each chapter due the next class unless otherwise noted. Please log into WorldClassroom by Friday, March 12th (to make sure there are no issues).
Lecture Week 2	Combined Readings	Understanding Cryptography: Chapters 2 (Stream Ciphers) and 3 (DES) The Code Book - Chapter 2 - Le Chiffre Ind'echiffrable
Lecture Week 3	Combined Readings	Understanding Cryptography: Chapter 4 (AES) and 5 (More About Block Ciphers) The Code Book - Chapter 3 - The Mechanization of Secrecy
Lecture Week 4	Combined Readings	Understanding Cryptography: Chapter 6 (Introduction to Public Key Cryptography) The Code Book - Chapter 4 - Cracking the Enigma
Lecture Week 5	Combined Readings	Understanding Cryptography: Chapter 7 (RSA) The Code Book - Chapter 5 - The Language Barrier Midterm Examination
Lecture Week 6	Combined Reading	Understanding Cryptography: Chapters 8 and 9 The Code Book - Chapter 6 - Alice and Bob Go Public
Lecture Week 7	Combined Readings	Understanding Cryptography: Chapters 10 and 11 The Code Book - Chapter 7 - Pretty Good Privacy
Lecture Week 8	Combined Readings	Understanding Cryptography: Chapter 12 The Code Book - Chapter 8 - Quantum Leap into the Future Research Paper Due
Lecture Week 9	Reading	Understanding Cryptography: Chapter 13 Semester Review Final Examination <u>ONLINE EVALUATION:</u> https://evaluation.webster.edu - <i>available weeks 8 & 9</i> Also available in WorldClassroom.

* Course Policies

Please silence all cell phones during class. Even while meeting remotely a ringing phone can be distracting.

Institutional Policies

Academic Policies

Academic policies provide students with important rights and responsibilities. Students are expected to familiarize themselves with all academic policies that apply to them. Academic policies for undergraduate students can be found in the Undergraduate Studies Catalog; graduate students should review the Graduate Studies Catalog.

Undergraduate Studies Catalog

The Undergraduate Studies Catalog contains academic policies that apply to all undergraduate students. The *academic policies and information* section of the catalog contains important information related to **attendance, conduct, academic honesty, grades, and more**. If you are an undergraduate student, please review the catalog each academic year. The current Undergraduate Studies Catalog is at:

<http://www.webster.edu/catalog/current/undergraduate-catalog/> (<http://www.webster.edu/catalog/current/undergraduate-catalog/>).

Graduate Studies Catalog

The Graduate Studies Catalog contains academic policies that apply to all graduate students. The *academic policies* section of the catalog contains important information related to **conduct, academic honesty, grades, and more**. If you are a graduate student, please review the catalog each academic year. The current Graduate Studies Catalog is at:

<http://www.webster.edu/catalog/current/graduate-catalog/> (<http://www.webster.edu/catalog/current/graduate-catalog/>).

Grading

The Grades section of the academic catalog outlines the various grading systems courses may use, including the information about the final grade reported for this class.

Undergraduate

<http://www.webster.edu/catalog/current/undergraduate-catalog/academic-policies.html#grading>
(<http://www.webster.edu/catalog/current/undergraduate-catalog/academic-policies.html#grading>).

Graduate

<http://www.webster.edu/catalog/current/graduate-catalog/academic-policies.html#grades>
(<http://www.webster.edu/catalog/current/graduate-catalog/academic-policies.html#grades>).

Incomplete

There are important policies that govern grades of Incomplete (I), including the circumstances under which Incomplete grades are granted, deadlines for completion, and consequences should the remaining course work not be completed. It is the responsibility of a student who requests an Incomplete to ensure that he/she understands and follows the policies.

Grade Appeals

Instructors are responsible for assigning grades, and student should discuss grade issues with the instructor. Policies and procedures for appealing grades are available in the appropriate catalog.

Academic Honesty Policy

Webster University is committed to academic excellence. As part of our Statement of Ethics, we strive to preserve academic honor and integrity by repudiating all forms of academic and intellectual dishonesty, including cheating, plagiarism and all other forms of academic dishonesty. Academic dishonesty is unacceptable and is subject to a disciplinary response. Students are encouraged to talk to instructors about any questions they may have regarding how to properly credit others' work, including paraphrasing, quoting, and citation formatting. The university reserves the right to utilize electronic databases, such as Turnitin.com, to assist faculty and students with their academic work.

The University's Academic Honesty Policy is published in academic catalogs:

Undergraduate

<http://www.webster.edu/catalog/current/undergraduate-catalog/academic-policies.html>
(<http://www.webster.edu/catalog/current/undergraduate-catalog/academic-policies.html>).

Graduate

<http://www.webster.edu/catalog/current/graduate-catalog/academic-policies.html>
(<http://www.webster.edu/catalog/current/graduate-catalog/academic-policies.html>).

As a part of the University commitment to academic excellence, the Academic Resource Center provides student resources to become better acquainted with academic honesty and the tools to prevent plagiarism in its many forms:

http://www.webster.edu/arc/plagiarism_prevention/ (http://www.webster.edu/arc/plagiarism_prevention/).

Statement of Ethics

Webster University strives to be a center of academic excellence. The University makes every effort to ensure the following:

- The opportunity for students to learn and inquire freely
- The protection of intellectual freedom and the rights of professors to teach
- The advancement of knowledge through scholarly pursuits and relevant dialogue

To review Webster University's statement of ethics, see the Undergraduate Studies Catalog and the Graduate and Studies Catalog:

Undergraduate

<http://www.webster.edu/catalog/current/undergraduate-catalog/overview.html#ethics>
(<http://www.webster.edu/catalog/current/undergraduate-catalog/overview.html#ethics>).

Graduate

<http://www.webster.edu/catalog/current/graduate-catalog/ethics.html> (<http://www.webster.edu/catalog/current/graduate-catalog/ethics.html>).

Contact Hours for this Course

It is essential that all classes meet for the full instructional time as scheduled. A class cannot be shortened in length. If a class session is cancelled for any reason, the content must be covered at another time.

Important Academic Resources

Academic Accommodations

Webster University makes every effort to accommodate individuals with academic/learning, health, physical and psychological disabilities. To obtain accommodations, students must identify themselves and provide documentation from a qualified professional or agency to the appropriate campus designee or the Academic ADA Coordinator at the main campus. The Academic ADA Coordinator may be reached at 314-246-7700 or disability@webster.edu (<mailto:disability@webster.edu>).

If you have already identified as a student with a documented disability and are entitled to classroom or testing accommodations, please inform the instructor of the accommodations you will require for this class at the beginning of the course.

Academic Resource Center

Additional support and resources may be accessed through the Academic Resource Center (ARC). Support and resources include academic counseling, accommodations, assistive technology, peer tutoring, plagiarism prevention, testing center services, and writing coaching. Visit www.webster.edu/arc (<http://www.webster.edu/arc>) or Loretto Hall 40 on the main campus for more information.

Student Success Portal

Webster University's Student Success Portal, powered by Starfish, is a communications tool to connect students with faculty members and campus support services. It allows faculty and staff members to communicate with you regarding academic achievements as well as areas where support may be helpful. You may use the portal to contact faculty and staff members for assistance and to arrange meetings. Activity in the portal will be communicated to your Webster University email account. The Student Success Portal is available via your course home page in WorldClassRoom or via Connections. Learn more about the Student Success Portal at <http://www.webster.edu/success/students.html> (<http://www.webster.edu/success/students.html>).

University Library

Webster University Library is dedicated to supporting the research needs and intellectual pursuits of students throughout the University's worldwide network. Resources include print and electronic books, journal articles, online databases, DVDs and streaming video, CDs and streaming music, datasets, and other specialized information. Services include providing materials at no cost and research help for basic questions to in-depth exploration of resources. The gateway to all of these resources and services is <http://library.webster.edu> (<http://library.webster.edu>). For support navigating the library's resources, see <http://libanswers.webster.edu/> (<http://libanswers.webster.edu/>) for the many ways to contact library staff.

Drops and Withdrawals

Drop and withdrawal policies dictate processes for students who wish to unenroll from a course. Students must take proactive steps to unenroll; informing the instructor is not sufficient, nor is failing to attend. In the early days of the term or semester, students may DROP a course with no notation on their student record. After the DROP deadline, students may WITHDRAW from a course; in the case of a WITHDRAW, a grade of W appears on the student record. After the WITHDRAW deadline, students may not unenroll from a course. Policies and a calendar of deadlines for DROP and WITHDRAW are at:

Undergraduate

<http://www.webster.edu/catalog/current/undergraduate-catalog/enrollment.html>
(<http://www.webster.edu/catalog/current/undergraduate-catalog/enrollment.html>).

Graduate

<http://www.webster.edu/catalog/current/graduate-catalog/enrollment.html> (<http://www.webster.edu/catalog/current/graduate-catalog/enrollment.html>).

Academic Calendar - <http://www.webster.edu/academics/academic-calendar/> (<http://www.webster.edu/academics/academic-calendar/>).

Current tuition rates, policies, and procedures, including details of pro-rated tuition refunds, are available in the "Tuition, Fees, and Refunds" section of Webster's Academic Catalogs:

Undergraduate

<http://www.webster.edu/catalog/current/undergraduate-catalog/tuition.html>
(<http://www.webster.edu/catalog/current/undergraduate-catalog/tuition.html>).

Graduate

<http://www.webster.edu/catalog/current/graduate-catalog/tuition.html> (<http://www.webster.edu/catalog/current/graduate-catalog/tuition.html>).

Student Handbook and Other Important Policies

Student handbook and other non-academic policies may apply to you and may impact your experience in this class. Such policies include the student code of conduct, privacy, technology and communications, and more. Please review the handbook each year and be aware of policies that apply to you. The handbook is available at:

<http://www.webster.edu/student-handbook/> (<http://www.webster.edu/student-handbook/>).

Sexual Assault, Harassment, and Other Sexual Offenses

Webster University makes every effort to educate the community to prevent sexual assault, harassment, and other sexual offenses from occurring, and is committed to providing support to those affected when this behavior does occur. To access information and resources or to review the Policy on Sexual Assault, Harassment, and Other Sexual Offenses, visit:

<http://www.webster.edu/sexual-misconduct/> (<http://www.webster.edu/sexual-misconduct/>).

Research on Human Subjects

The Webster University Institutional Review Committee (IRB) is responsible for the review of all research on human subjects. The IRB process applies to all Webster University faculty, staff, and students and must be completed prior to any contact with human subjects. For more information on the IRB, visit:

<http://www.webster.edu/irb/index.html> (<http://www.webster.edu/irb/index.html>).

Course Evaluations

At the end of this course, you will have the opportunity to provide feedback about your experience. Your input is extremely valuable to the university, your instructor, and the department that offers this course. Please provide your honest and thoughtful evaluation, as it helps the university to provide the best experience possible for all of its students.

Important Technology Information

Connections Accounts

Webster University provides all students, faculty, and staff with a University email account through Connections. Students are expected to activate their Connections account and regularly check incoming University email. Students may choose to have their University email forwarded to an alternate email address. Connections account holders can call the Help Desk (314-246-5995 or toll free at 1-866-435-7270) for assistance with this setup. Instructions are also provided on the Information Technology website at:

<http://www.webster.edu/technology/service-desk/> (<http://www.webster.edu/technology/service-desk/>).

WorldClassRoom

WorldClassRoom is Webster's Learning Content Management System (LMS). Your instructor may use WorldClassRoom to deliver important information, to hold class activities, to communicate grades and feedback, and more. WorldClassRoom is available using your Connections ID at:

<https://worldclassroom.webster.edu/> (<https://worldclassroom.webster.edu/>).

Webster Alerts

Webster Alerts is the University's preferred emergency mass notification service, available free to current students, faculty and staff at all US campuses. By registering a valid cell phone number and email address, you will receive urgent campus text, voice mail and email communications. Valuable information concerning a range of incidents affecting you - from weather-related campus closures, class delays and cancellations, to more serious or life-threatening events - are immediately and simultaneously delivered through multiple communication channels. To register for Webster Alerts, visit:

<http://www.webster.edu/technology/services/webster-alerts/> (<http://www.webster.edu/technology/services/webster-alerts/>).

Campus Information

Due to the Education Centers not re-opening in the DC region for this term *please* meet via Zoom for the Spring 2 term.

Instructors will post the meetings in WorldClassroom/Canvas for students to log in each week (added security measure). On the left side with all the hyperlinks there will be one for Zoom.

We recommend **Chrome** for the browser and please mute yourself when not speaking, also only you are able to unmute yourselves in Zoom. If there are many participants it also might be wise to disengage video too (or if bad weather) if low band width messages continually appear.

Webster University: Joint Base Myer/Henderson Hall:

Phone (844) 347-0568

hendersonhall@webster.edu

Additional Items

Emerson Library: library.webster.edu

There is a live chat feature - home page, contact a librarian (middle of page, middle box): Chat with a librarian on left side (might have to scroll down a bit) - accessible 24 hours a day.

The WSBT subject librarian is:

Business & Management	Mary Anne Erwin	800-985-4279	maerwin@webster.edu
-----------------------	---------------------------------	--------------	--

Please use these excellent resources