IS 401 – Cryptography and Network Security

***DONNELLY COLLEGE***

Instructor:

Term

Day/Time

Room

3 Credit Hours

**INSTRUCTOR INFORMATION:**

Name:

Office hours:

Telephone:

E-mail address:

Web site address: [www.donnelly.edu](http://www.donnelly.edu)

**COURSE DESCRIPTION:**

This course explores cybercrime relating history, environment, legal issues, and future of network and computer crime. In this course, students will investigate different types of computer criminals, research criminal motivation and their methods of attack. Weekly case studies will be used to analyze the present of cyber-intelligence, cyber espionage, and cyber-attacks throughout the United States and the world.

**PREREQUISITES:** Senior Level standing and IS 303

**REQUIRED TEXTBOOK & SUPPLIES:**.

**IS 401 Text**: Cryptography and Network Security Principles and Practice

By Stallings

ISBN: 9781644591888

Publisher: UCertify

**PHILOSOPHY OF GENERAL EDUCATION:**

Donnelly College has consistently maintained a strong commitment to the liberal arts and sciences as a foundation for a complete education. The faculty strongly believes that the liberal arts and sciences provide the context through which students can engage with the larger questions about students’ place in the world and their pursuit of truth. Therefore, the College’s general education requirements are designed to ensure that liberal arts and sciences graduates develop a breadth of content knowledge and the skills and abilities, which will enable them to become educated participants in a diverse global community.

**DONNELLY COLLEGE LEARNING OUTCOMES:**

1. **Communication Skills:** Students will communicate effectively in writing and speaking.
2. **Technology and Information Literacy Skills:** Students will demonstrate proficiency in information literacy skills.
3. **Symbolic Problem Solving:** Students will demonstrate competency in qualitative and quantitative problem solving.
4. **Analytical Thinking:** Students will employ reflective thinking to evaluate diverse ideas in the search for truth.
5. **Personal and Interpersonal Skills:** Students will develop an understanding across cultural differences locally, nationally, and internationally.
6. **Academic Inquiry:** Students will engage independently and effectively in lifelong learning.
7. **Values:** Students will demonstrate moral and ethical behavior in keeping with our Catholic identity.

**PROGRAM LEARNING OUTCOMES:**

In addition to the general education learning outcomes – communication skills, technology and information literacy skills, symbolic problem solving, analytical thinking, personal and interpersonal skills, academic inquiry, and values – upon successful completion of the Bachelor of Science in Information Systems degree, students will demonstrate:

1. An ability to communicate effectively on multidisciplinary teams with a wide range of people. 2. An ability to use the techniques, skills, and modern computing tools necessary for technological practice.

3. The aptitude to analyze qualitative and quantitative data to make informed decisions.

4. An ability to ethically design a system, component, or process to meet desired needs within realistic constraints.

5. The capacity to function effectively on teams that understand the impact technology has in a local, national, and global context.

6. Recognition of the need for, and willingness to engage in life-long learning through a continuous investigation of contemporary issues.

7. The capacity to make informed decisions in computing practice based on an understanding of professional, legal, and ethical responsibilities.

**STUDENT LEARNING OUTCOMES:**

1. Students will have an ability to understand and explain the basics of Cryptography and Network Security.
2. Students will have an ability to explain the advantages of Cryptography and solid Network Security practices.
3. Students will have an ability to explain the issues within improper use of Cryptography and Network security.
4. Students will have an understanding of the influence of cryptography and Network Security in a professional setting.
5. Students will have an understanding on how network systems are organized and how cryptography is utilized.
6. Students will have an understanding of theories of Cryptography and Network Security.
7. Students will have an ability to formulate criteria for new Cryptography and Network Security Solutions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Donnelly College****Learning Outcomes** | **Program Learning Outcomes1** | **Student Learning Outcomes2** | **Application and Assessment3** |
| Students will communicate effectively in writing and speaking. | *The student will demonstrate academically accepted written and oral communications* | Students will have an ability to explain the basics of Cryptography and Network security. | Students will achieve an 80% passing average on projects   |
| Students will demonstrate proficiency in information literacy skills. | *The student will demonstrate the capacity to understand basic cypher codes and computerized Cryptography along with basic Network Security protocol.* | Students will have an ability to understand basic Cryptography Cypher codes and basics of Network Security. | Students will achieve an 80% passing average on Labs and exercises in UCertify. |
| Students will demonstrate competency in qualitative and quantitative problem solving. | *The student will demonstrate an aptitude to analyze qualitative and quantitative data to make informed decisions.*  | Students will have an understanding as to the solving of basic cypher code. Students will have an ability to trouble shoot basic Network Security issues.  | Students will achieve an80% passing average on Labs an Exercises assigned in UCertify as well as instructor provided cypher codes. |
| Students will employ reflective thinking to evaluate diverse ideas in the search for truth. | *The student will demonstrate an ability to design a system, component, or process to meet desired needs within realistic constraints.* | Students will have an understanding of the importance of Cryptography and Network security in a professional setting.  | Students will achieve an80% passing average on Labs an Exercises assigned in UCertify as the design of a basic Network Security outline.  |
| Students will develop an understanding across cultural differences locally, nationally, and internationally. | *The student will demonstrate the capacity to function effectively on teams that understand the impact technology has in a global, economic, environmental, and societal context.* | Students will have an ability to independently judge criteria for Network Security layouts as well as collaborate on the solve of various cypher codes.  | Students will achieve an80% passing average on Labs an Exercises assigned in UCertify as well as the creation and solution of a basic cypher code. |
| Students will engage independently and effectively in lifelong learning. | *The student will demonstrate an understanding of their leadership style and application of that style to various situations.* | Students will have an ability to explain the competitive advantages utilizing Cryptography and a solid Network Security foundation.  | Students will achieve an80% passing average on Labs an Exercises assigned in UCertify. |
| Students will demonstrate moral and ethical behavior in keeping with our Catholic identity. | *The student will demonstrate service leadership to others by participating in a service-leadership initiative* | Students will have the ability to lead a team in the formation of a new network security outline. | Students will achieve an80% passing average on Labs an Exercises assigned in UCertify. |

**COURSE REQUIREMENTS:**

**Reading the Text**: Cryptography and Network Security can be a very interesting course, but it is sufficiently technical in nature to require the student to keep current. **Review of the text and UCertify prior to class is Mandatory.**

**Attendance and Participation/Online Discussions –** You will be expected to show your attendance through online class discussions. You will receive up to 10 points per each online class discussion, but only if you are participating in the activities and discussions. The points cannot be made up after the discussion closes.

**Syllabus Quiz – Will be taken the first day of class**

**Power Point**: Students will be required to create one cohesive power point presentation with references. The presentation will be over one company, how the company functioned prior to an ERP implementation and the results and changes in business process after the implementation. It must include a cost analysis prior to and after implementation. There is not a set slide length for the presentation, however, to effectively communicate the need a minimum of 12 slides is suggested. The inclusion of graphs to support the research is a bonus.

**Examinations**: The course will cover several chapters in the text in a midterm exam and a final exam. These exams could be paper and pencil responses, take home test, online or a project.

|  |
| --- |
| *Rubric Template for the term paper. Evaluate a situation at work from a complete human resource perspective. The paper must include a motivational component.* |
|   | Points Possible  | Points Possible | Points Possible | Points Possible | **Points Earned** |
| **Criteria #1****Spelling/ grammar** 10% | Proper grammar and spelling throughout paper20-15 | A few grammatical errors in paper14-10 | Acceptable 9-4 | Paper is poorly written and difficult to read 0 | \_\_\_\_ |
| **Criteria #2****HR principles applied** **60%** | Demonstrates complete understanding of HR and lessons applied from 180-150 | Demonstrates considerable mastery of class material and application149-130 | Demonstrates partial understanding of material and its application129-100 | Demonstrates little or no understanding of material application 99-0 | \_\_\_\_\_ |
| **Criteria #3****Motivational component** 30% | Motivational concept clearly understood and demonstrated60-45 | Demonstrates partial understanding of concepts44-30 | Acceptable29-15 | Little or no understanding of motivational concepts 14-0 | \_\_\_\_\_ |

**Online Discussion Rubric**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Points** | 10 | 7 | 3 | 0 |
| **Quality of Post** | Appropriate comments: thoughtful, reflective, and respectful of other’s postings. | Appropriate comments and responds respectfully to other's postings. | Responds, but with minimum effort. (e.g. "I agree with Bill"). | No posting. |
| **Relevance of Post** | Posts topics related to discussion topic; prompts further discussion of topic. | Posts topics that are related to discussion content. | Posts topics which do not relate to the discussion content; makes short or irrelevant remarks. | No posting. |
| **Contribution to the Learning Community** | Aware of needs of community; attempts to motivate the group discussion; presents creative approaches to topic. | Attempts to direct the discussion and to present relevant viewpoints for consideration by group; interacts freely. | Does not make effort to participate in learning community as it develops. | No feedback provided to fellow student. |

**GRADING POLICY:**

Attendance and Participation 45 @ 10 points per class 450

Weekly questions/labs 16 @ 20 points 300

Exams: 2 @ 100 points each Midterm & Final 200

Total available points 950

**GRADING SCALE:**

A: 90%-100% 1053-1170

B: 80%-89% 936-1052

C: 70%-79% 819-935

D: 60%-69% 702-818

F: Below 60% 701 points and below

**ACADEMIC INTEGRITY:** “Academic integrity is to be maintained at all times to insure genuine educational growth. Cheating and plagiarism in all forms, therefore, will be subject to disciplinary action. Serious infractions will be reviewed by an ad hoc committee, appointed by the appropriate dean. Appropriate sanctions will be imposed.”

**PLAGIARISM:** Plagiarism-the appropriation or imitation of the language or ideas of another person and presenting them as one’s original work-sometimes occurs through carelessness or ignorance. Students who are uncertain about proper documentation of sources should consult their instructors.

**ACCOMMODATIONS:** In compliance with the Americans with Disabilities Act, Donnelly College will make every attempt to provide equal access for persons with disabilities. Students in need of accommodations must request them in writing from the Vice President of Academic Affairs.

**CIVILITY & DECORUM:** As noted in its Code of Conduct, Donnelly College is committed to maintaining an overall atmosphere of civility and respect. Civility and decorum both inside and outside the classroom are fundamental foundations of the values at Donnelly College. Classroom discussions and interactions outside the classroom will at all times be focused on the learning process and should always be respectful of both students and faculty. In open discussions of ideas and issues, disagreements should focus on ideas and facts. Name calling and assaults (either in person or on-line) will not be tolerated. Should any problems occur, the instructor should be notified immediately. Those who do not comply with civility and decorum requirements may be subject to a grade reduction and/or other sanctions up to and including dismissal from Donnelly College.

**ATTENDANCE AND ASSIGNMENTS DUE POLICIES:** Experience and research have shown that students who do not attend class tend to have lower grades. Communication involves collaboration with peers. Learning is cumulative. Every lesson builds on those that precede it.

**The student will be expected to demonstrate maturity and responsibility in attendance and in submission of assignments.**

1. Attendance will be taken each day by the instructor.
2. Avoid absences—schedule appointments outside of class time.
3. If you must be absent for Donnelly-sponsored events, you may **turn in assignments early,** if sponsors (Student Senate, TRIO, etc…) notify me.
4. Late assignments will **not** be accepted for a grade, unless you have proper documentation i.e. doctors excuse.
5. **Missing a test, will require you to show me documentation of verified illness (NO EXCEPTIONS).** Contact me, outside of class time, to discuss your reasons for the absence. Talk to me so that we can arrange a schedule for you to catch up.
6. Keep a schedule of assignments with your text or check Canvas for due dates. Some of those will change as semester progresses. Keep your schedule revisions up-to-date.
7. Making up pop quizzes or in class assignments **will be impossible.**
8. Make up tests **(for those with proper documentation ONLY),** will be coordinated with the instructor, but **any exam taken late, for ANY reason, will be worth 20% LESS.** **No one will be permitted to make up more than one late exam.**
9. I will not use class time to review material missed because of absences. Use your textbook. Ask other students or me for help and explanations outside of class time.
10. If, for any reason, you are unable to complete this course, **YOU must officially withdraw**. Students who stop attending or who are **absent** **more than 6 courses total (two weeks of classes), may be administratively withdrawn from the course.** Check the Donnelly College Calendar for **last date to withdraw (see policy below).**
11. The schedules for finals will be posted. Check the calendar for dates and times. **All students must take the final.**

**Exceptions to the above policies will be rare and at the instructor’s discretion.**

**WITHDRAWAL FROM COURSES OR FROM SCHOOL:** It is the responsibility of the student to withdraw from class. If a student decides to withdraw from a class, ideally, they should see an advisor and the financial aid staff before taking the withdrawal form to the Registrar's office for processing.  However, any verifiable contact (e-mail, fax, phone, mail, etc.) with authorized college personnel expressing the student's intent to withdraw from a class will be honored.

If students withdraw before they have earned their financial aid, they will owe Donnelly College a debt for the unearned portion of the financial aid as well as for any unpaid balances (subject to the College's refund policy). Not attending class is not a withdrawal from class.

**Donnelly College reserves the right to withdraw a student from class(es) if the student does not meet their financial obligations, including two missing or incomplete payments, or loss of financial aid.** Faculty may initiate an administrative withdrawal on the basis of non-attendance. In extreme circumstances (i.e. a disciplinary problem), the Vice President of Academic Affairs may initiate an administrative withdrawal. The student remains responsible for the tuition owed in this instance.

The deadlines for withdrawing from classes are as follows:

|  |  |
| --- | --- |
| 14 to 16 weeks | 3 weeks before the end of the class |
| 6 to 8 weeks                | 7 weekdays before the end of class |
| 4 to 5 weeks                | 4 weekdays before the end of class |
| Less than 4 weeks | Withdrawals are not allowed |

Withdrawal deadline dates will be published in the academic calendar.

**CONTACT PERSONS:** It is recommended that you record the names, e-mail addresses, and phone numbers of at least 2 other classmates so that you can contact someone if you have questions.

**CLASSROOM COURTESY:** Turn off all cell phones while in the classroom (if you are expecting an important call, please set your phone to vibrate and excuse yourself from the classroom to take the call). Texting in class will not be tolerated. Anyone caught texting during class/lecture will be asked to leave the classroom for that day.

**GROUP WORK:** Working with other students in study groups is an extremely effective means of studying. Not everyone in the study group needs to be at the same proficiency level: teaching others is a very powerful way to learn material for yourself. Make sure, however, that you do not simply copy another’s homework and turn it in as your own. When working in groups all participants must vary their work so that each assignment reflects individual work.

**CREDIT HOUR POLICY: EXPECTATION FOR STUDENTS:** Donnelly College’s assignment of credit hours shall conform to commonly accepted practices in higher education and the federal definition of a credit hour. For each credit hour, students should anticipate spending a minimum of 150 minutes per week based on a 16-week semester. The distribution of this time will vary based on the course and delivery method, but could include direct faculty instruction, classroom activities, web-based activities, laboratory work, research, writing papers and reports, reading text and articles, internship hours, clinical hours, studio work, or class and assessment preparation.

**TENTATIVE COURSE CALENDAR:**

The schedule is subject to change based on the progress or needs of the class.

|  |  |  |
| --- | --- | --- |
| **Week #** | **Content to Be Covered[[1]](#footnote-1)** | **Dates** |
| 1 | **Information and Network Security Concepts*** Cybersecurity, Information Security, and Network Security
* The OSI Security Architecture
* Security Attacks
* Security Services
* Security Mechanisms
* Cryptography
* Network Security
* Trust and Trustworthiness
* Standards

**Introduction to Number Theory*** Divisibility and The Division Algorithm
* The Euclidean Algorithm
* Modular Arithmetic
* Prime Numbers4
* Fermat’s and Euler’s Theorems
* Testing for Primality
* The Chinese Remainder Theorem

Discrete Logarithms | 8/16 & 8/18/2021 |
| 2 | **Classical Encryption Techniques*** Symmetric Cipher Model
* Substitution Techniques
* Transposition Techniques

**Block Ciphers and the Data Encryption Standard*** Traditional Block Cipher Structure
* The Data Encryption Standard
* A DES Example
* The Strength of DES
* Block Cipher Design Principles
 | 8/23 & 8/25/2021 |
| 3 | **Finite Fields*** Groups
* Rings
* Fields
* Finite Fields of the Form GF(p)
* Polynomial Arithmetic
* Finite Fields of the Form GF (2n)

**Advanced Encryption Standard*** Finite Field Arithmetic
* AES Structure
* AES Transformation Functions
* AES Key Expansion
* An AES Example
* AES Implementation
 | 8/30 & 9/1/2021 |
| 4 | **\*9/6 no class Labor Day****Block Cipher Operation*** Multiple Encryption and Triple DES
* Electronic CodeBook
* Cipher Block Chaining Mode
* Cipher Feedback Mode
* Output Feedback Mode
* Counter Mode
* XTS-AES Mode for Block-Oriented Storage Devices
* Format-Preserving Encryption

**Random Bit Generation and Stream Ciphers*** Principles of Pseudorandom Number Generation
* Pseudorandom Number Generators
* Pseudorandom Number Generation Using a Block Cipher
* Stream Ciphers
* RC4
* Stream Ciphers Using Feedback Shift Registers

True Random Number Generators | 9/06 – 9/08/2021 |
| 5 | **Public-Key Cryptography and RSA*** Principles of Public-Key Cryptosystems
* The RSA Algorithm

**Other Public-Key Cryptosystems*** Diffie–Hellman Key Exchange
* Elgamal Cryptographic System
* Elliptic Curve Arithmetic
* Elliptic Curve Cryptography
 | 9/13 & 9/15/2021 |
| 6 | **Cryptographic Hash Functions*** Applications of Cryptographic Hash Functions
* Two Simple Hash Functions
* Requirements and Security
* Secure Hash Algorithm (SHA)
* SHA-3

**Message Authentication Codes*** Message Authentication Requirements
* Message Authentication Functions
* Requirements for Message Authentication Codes
* Security of MACs
* MACs Based on Hash Functions: HMAC
* MACs Based on Block Ciphers: DAA and CMAC
* Authenticated Encryption: CCM and GCM
* Key Wrapping
* Pseudorandom Number Generation Using Hash Functions and MACs
 | 9/20 & 9/22/2021 |
| 7 | **Digital Signatures*** Digital Signatures
* Elgamal Digital Signature Scheme
* Schnorr Digital Signature Scheme
* NIST Digital Signature Algorithm
* Elliptic Curve Digital Signature Algorithm
* RSA-PSS Digital Signature Algorithm

**Lightweight Cryptography and Post-Quantum Cryptography*** Lightweight Cryptography Concepts
* Lightweight Cryptographic Algorithms
* Post-Quantum Cryptography Concepts

Post-Quantum Cryptographic Algorithms | 9/21 & 9/29/2021 |
| 8 | **Midterms** | 10/4 & 10/6/2021 |
| 9 | **Cryptographic Key Management and Distribution*** Symmetric Key Distribution Using Symmetric Encryption
* Symmetric Key Distribution Using Asymmetric Encryption
* Distribution of Public Keys
* X.509 Certificates
* Public-Key Infrastructure

**User Authentication*** Remote User-Authentication Principles
* Remote User-Authentication Using Symmetric Encryption
* Kerberos
* Remote User-Authentication Using Asymmetric Encryption
* Federated Identity Management
 | 10/11 & 10/13/2021 |
| 10 | **Transport-Level Security*** Web Security Considerations
* Transport Layer Security
* HTTPS
* Secure Shell (SSH)

**Wireless Network Security*** Wireless Security
* Mobile Device Security
* IEEE 802.11 Wireless LAN Overview

IEEE 802.11i Wireless LAN Security | 10/18 & 10/20/2021 |
| 11 | **Electronic Mail Security*** Internet Mail Architecture
* Email Formats
* Email Threats and Comprehensive Email Security
* S/MIME
* DNSSEC
* DNS-Based Authentication of Named Entities
* Sender Policy Framework
* Domainkeys Identified Mail
* Domain-Based Message Authentication, Reporting, and Conformance

**IP Security*** IP Security Overview
* IP Security Policy
* Encapsulating Security Payload
* Combining Security Associations
* Internet Key Exchange
 | 10/25 & 10/27/2021 |
| 12 | **Network Endpoint Security*** Firewalls
* Intrusion Detection Systems
* Malicious Software
* Distributed Denial of Service Attacks

**Cloud Security*** Cloud Computing
* Cloud Security Concepts
* Cloud Security Risks and Countermeasures
* Cloud Security as a Service
* An Open-Source Cloud Security Module
 | 11/01 & 11/03/2021 |
| 13 | **Internet of Things (IoT) Security*** The Internet of Things
* IoT Security Concepts and Objectives

An Open-Source IoT Security Module | 11/08 & 11/10/2021 |
| 14 | Student lead Cypher Codes | 11/15 & 11/17/2021 |
|  | Classes out for Thanksgiving | 11/24 - 11/26 |
| 15 | Student lead Network Security Outline | 11/29 & 12/1/2021 |
| 16 | Final review / start final | 12/6/2021 |
| 16 | **Final Course Project Is Due** | **12/8/2021** |

1. Weekly announcements, reading materials, homework, and projects are posted on Canvas. [↑](#footnote-ref-1)