INA 4381 Introduction to Cryptology

Course Description/Overview

This course's ultimate objective is to introduce the student to the world of codes and ciphers. This course will rely on the long history of cryptology, from 1900 B.C.E. to present day. This course introduces to students to several methods of both manual encryption and decryption and methods used today to ensure personal information is encrypted in both military and civilian applications.

Click this link for a printable version of the syllabus.

Course Prerequisites:

While there are no prerequisites, the course materials, assignments, learning objectives and expectations in this upper level undergraduate course assume that the student has completed all lower level general education coursework. Such coursework is necessary to develop research, writing, and critical thinking skills. Students who have not fulfilled all general education requirements will be at a great disadvantage and should strongly consider completing those requirements prior to registering for this course.

Course Bibliography and Required Readings:

The following textbook is required for this course. Other readings are assigned each week and are provided to you via a link in the course materials. Additionally, where possible, videos are utilized to enhance student learning.

- Singh, Simon. *The Code Book: The Secrets Behind Codebreaking*. New York: Ember, 2016. ISBN: 9780375890123
- Provided Texts

1. Basic Cryptanalysis Field Manual (FM 34-40-2)
2. History of Encryption White Paper from SANS.org
3. Military Cryptanalysis War Department Military Cryptanalysis

Course Objectives/Learning Outcome

Objectives: As a result of completing this course, the student will be able to:

- **Objective One**: Demonstrate a knowledge of the definition of cryptology
- **Objective Two:** Demonstrate a knowledge of the history of cryptology before the U.S. Civil War.
- **Objective Three:** Demonstrate a knowledge of the history of cryptology after the U.S. Civil War to the present.
- **Objective Four:** Demonstrate a working knowledge of encoding to include steganography.
- **Objective Five:** Demonstrate a working knowledge of how to decode a message.
- **Objective Six:** Demonstrate a basic working knowledge of the operations of a 10 by 10 coded matrix.

Learning Outcome: Students have a right to know what instructors expect them to learn from a course of instruction and how their learning will be measured. This course establishes several learning outcomes that are measured subjectively. When you finish this course you should be able to:

1. Describe the history of cryptology.

2. Describe why cryptology was needed, and is still in use today.

3. Discuss the use of military cryptology.

4. Describe the method of both encoding and decoding.

Grading Policies/Assessment of Learning

A Note on Grades: ISSA 4307 is a colloquium (meaning a group discussion, from the Latin Colloqui – to talk together—to have a conversation). As such, weekly participation in the discussion threads is expected and forms part of the grade. Final grades are composed as follows:

Assignment	Percent of Grade	Due
Participation in the Discussion Board	30%	Weekly for weeks 1 – 3 and 5-7. Weeks 4 and 8 won't have discussion forums.

First Essay	30%	**11:59pm Central Time of Sunday end of Lesson 4**. at least 1200 words in length
Final Essay	40%	**11:59pm Central Time of Thursday of Lesson 8.** at least 1500 words in length

Knowledge of course objectives and learning outcomes will be assessed through:

Weekly Discussion Questions

Weekly discussion questions allow the student to demonstrate comprehension of lesson materials by preparing a response to a discussion question(s) posed by the instructor. The student response is assembled from knowledge gained through course materials and independent research. All students should follow the "General Rules for Discussion Questions Posts" below. Failing to follow these rules and guidelines may result in score deductions. Formal grading of weekly discussion questions will be completed using the Discussion Question Grading Rubric.

General Rules for Discussion Question Posts:

All students MUST participate. Failing to participate may result in a failing grade for the course. Students must post a response to the instructors' weekly question by 11:59 p.m. CST on Thursday of each week and must respond to a minimum of two other students' post by 11:59 p.m. CST on Sunday of each week.

Engage in an honest and forthright discussion, backing your position with proper references. There are no "correct" answers in the discussion area.

Stating a position on an issue without providing a reference to source materials to back up your position is "simply your opinion." Such opinion statements are not appropriate in an academic setting.

Avoid repeating the assigned readings in your own words. Use assigned readings as one of your resources, not as the single source for your post.

Avoid plagiarism - paraphrasing a source document is plagiarism if you do not give the author due credit.

Research Paper (1)

A research paper on a topic relating to current or historical use of cryptology is due at the end of Week 4. The research paper assignment is due no later than 11:59 p.m. CST on Sunday of Week 4. Student performance on the research paper will be evaluated using the Research Paper Grading Rubric. Late papers will be assessed a point reduction (10 Points) for each day the paper is late.

Your opinion will not be a determining factor in your grade. Your grade is determined by how well you support your argument utilizing the materials discussed in the course, along with independent research and reference materials that you locate on your own. DO NOT simply repeat the course materials in your research paper. While you may use course resources for your research paper, you must provide reference to a minimum of 4 resources that are independent of the course materials.

The first paper must be at least 1200 words in length. It must have a title page that includes the title, course name and number, instructor's name, author's name, and date. Use standard 1 inch margins on all sides, 12 point Arial or Times New Roman font, and standard double-spacing. An abstract is NOT required. Cite your references in EVERY instance and include a properly formatted reference list at the end of the paper. Use at least four sources for the first paper, with relevant citations to those sources.

CMS (Chicago Manual Style) is the preferred format for this course. To access the Chicago Style guide, go to: http://www.chicagomanualstyle.org.

Every writing assignment should be submitted as a Microsoft Word. If you do not have Microsoft Office, then copy the text you have written directly into the assignment section of Blackboard during the appropriate week. Or go to the library and use their computers. DO NOT submit writing assignments in Word Perfect, Microsoft Works, or some e-mail format. They will not be accepted.

Outline for the Research Paper:

Introduction - The first section of any research paper should be the introduction. The introduction describes the general issues that the paper will address. Within the introduction you must state a theory, thesis or topic for the paper. The introduction provides the reader with an understanding of the basic subject of your paper and the main points that you will make about your chosen topic. The

introduction should express the broad connections that tie together the more specific points you will make and observations that you will document later in the paper. The introduction should provide the reader with a sense of what they will learn about your topic through reading your paper.

Body - The sections and paragraphs within the body of your paper should always tie back to your main topic. Do not continually re-state your main topic, but ensure that the reader knows how the sub-topic in each section or paragraph develops, supports or challenges the main topic of your paper. To maintain continuity in your argument, make sure that you create effective transitions between each section and paragraph. An easy way to accomplish this is to make sure that the first lines of each new section or paragraph reflect back on the previous section or paragraph and that all are in logical order.

Conclusion - Your conclusion section should reflect back on what you have written, summarize your findings, identify any weaknesses in your argument, and point the way for you and/or the reader to complete further assessment on the topic.

First Paper Assignment: Lesson 4:

The Mid-term assignment is an essay. The requirements are:

The assignment is to write an essay:

What is the history of PGP, such as why was it written, and released? What are the strengths and weaknesses of PGP?

All course materials and readings may be used as references for this essay. While there is no minimum number of references required, you must document your evidence completely and support your arguments thoroughly.

*Essay will be turned in to the professor via the Blackboard Assignment system. DO NOT USE BLACKBOARD MESSENGER OR EMAIL.

A video that describes how to upload assignments in Blackboard can be viewed by clicking this link: Uploading Blackboard Assignments - video

A printable version of these instructions can be viewed by clicking this link: Uploading Blackboard Assignments - PDF

Students will not present their essay to their fellow students.*

- **Type**: Individual Essay
- **Format**: All Margins one-inch
- **Format**: Double Spaced, 12 point, Times New Roman font
- **Length:** Five to Seven pages (NOT INCLUDING TITLE PAGE, REFERENCES, OR CITATIONS)
- **Due**: Thursday of week 4 before 11:59 p.m. Central Standard Time.
- **Please have a cover page for this assignment.** Ensure your name appears on both the cover page and on the name of the file, e.g., Smith_4381_Midterm.doc.
- **Resources:** You must cite a minimum of five different references in your essay, either from course materials or additional references (Wikipedia, blogs, and similar sources are NOT acceptable as sources).
  Any material to include, but not limited to, course readings and discussions. Adhere to bibliographic and citation guidelines.
- Complete instructions and guidance on bibliography and citation guidelines should adhere to the Chicago Manual of Style 16th Edition.

FINAL ASSIGNMENT

The final assignment is not a research paper, rather the final project will use methods discussed in lessons 5, 6 and 7.

Using the 10 by 10 matrix given in lesson 5, and using a steganography picture, decode the instructions contained in the image. The final instructions will consist of decoding the message in the image, following the instructions, and writing a 500 word paper about a particular topic found in your text book. The assignment requirements are:

- **Format**: All Margins one-inch
- **Format**: Double Spaced, 12 point, Times New Roman font
- **Length:** Five Hundred words (NOT INCLUDING TITLE PAGE, REFERENCES, OR CITATIONS)
- **Due**: Wednesday of week 4 before 11:59 p.m. Central Standard Time.
- **Please have a cover page for this assignment.** Ensure your name appears on both the cover page and on the name of the file, e.g., Smith_4381_Final.doc.
- **Resources:** You must cite a minimum of one reference in your essay, from your textbook. (Wikipedia, blogs, and similar sources are NOT acceptable as sources).
  Any material to include, but not limited to, course readings and discussions. Adhere to bibliographic and citation guidelines.
  Complete instructions and guidance on bibliography and citation guidelines should adhere to the Chicago Manual of Style 16th Edition. Ten point reduction will be assessed for each day the second paper is late.

Rubrics

Discussion forums and writing assignments will be graded using a standardized rubric. It is recommended that you be familiar with these grading criteria and keep them in mind as

you complete the writing assignments. There are two rubrics. Click the link to download the PDF document:

Discussion Rubric
Writing Assignment Rubric

Angelo State University employs a letter grade system. Grades in this course are determined on a percentage scale:

A = 90 – 100 %
B = 80 – 89 %
C = 70 – 79 %
D = 60 – 69 %
F = 59 % and below.

Course Organization/Learning Outcomes/and Required Readings:

Lesson 1: Theory of cryptology: including definitions, and usage.

Lesson 2: History of cryptology from B.C.E to the U.S Civil War

Lesson 3: History of cryptology from the U.S. Civil War to present

Lesson 4: Mid-term essay covering the history of cryptology from Lessons 2 and 3 (Note: your first paper is due midnight of Week 4).

Lesson 5: Encoding a message into an encrypted message. Steganography will be introduced in this lesson.

Lesson 6: Decoding a message into a readable format. Decoding of a steganography message from previous message will be demonstrated

Lesson 7: Practice of encoding and decoding messages from previous weeks in preparation for the final decoding messages

Lesson 8: A rather lengthy message will be posted, in an image, and the final will be based on the students ability to perform the action into readable format. (Note: your final is due midnight Wednesday night of Week 8).

Communication

Participation

In this class everyone, brings something to the table. Your ideas and thoughts do count, not only to me, but the entire class. Feel free to ask questions either via e-mail or the discussion board. Check the discussion board regularly. Many student questions are applicable to the class as a whole, as are the responses. You may be surprised how many of your classmates have the same questions and concerns as you. I may simply post your particular question on the discussion board and allow your classmates to provide the answer through their own posts.

To some, this may be their first online class and naturally, it could seem somewhat intimidating. As a class, we are together to help each other with this learning process and share our collective knowledge on how best to communicate; how to resolve technical issues that may arise (if we have the expertise), and to assist each other to find answers to our questions. We will learn and work as a team.

Courtesy and Respect

Courtesy and respect are essential ingredients to this course. We respect each other's opinions and respect their point of view at all times while in our class sessions. The use of profanity & harassment of any form is strictly prohibited (Zero Tolerance), as are those remarks concerning one's ethnicity, life style, race (ethnicity), religion, etc., violations of these rules will result in immediate dismissal from the course.

Netiquette

The on-line setting of our course promotes the advancement of knowledge through positive and constructive debate. Classroom based discussions between instructors and students and among students has traditionally been guided by the instructor. Discussions via the Internet, however, can occasionally devolve into insults and improper comments before the instructor has a chance to intervene.

Such activity and the failure to use proper etiquette and manners ARE NOT ACCEPTABLE in an academic setting and such inappropriate conduct IS NOT TOLERATED. Basic academic rules of good behavior and proper "Netiquette" are required and must prevail. Our on-line classroom is a place to enjoy the excitement of learning and does not include room for personal attacks on others or student attempts to demean or restrict the discussion of others. Note about the use of humor: Despite the best of intentions, jokes and especially- satire can easily be lost or taken seriously. Avoid the use of humor and/or satire in our academic setting.

Office Hours/Contacting the Instructor

See the Instructor Information section for contact information.

University Policies

Academic Integrity Angelo State University expects its students to maintain complete honesty and integrity in their academic pursuits. Students are responsible for understanding and complying with the university Academic Honor Code and the ASU Student Handbook.

Accommodations for Disability
ASU is committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs or activities of the university, or be subjected to discrimination by the university, as provided by the Americans with Disabilities Act of 1990 (ADA), the Americans with Disabilities Act Amendments of 2008 (ADAAA), and subsequent legislation.

Student Affairs is the designated campus department charged with the responsibility of reviewing and authorizing requests for reasonable accommodations based on a disability, and it is the student's responsibility to initiate such a request by emailing studentservices@angelo.edu, or by contacting:

Office of Student Affairs
University Center, Suite 112
325-942-2047 Office
325-942-2211 FAX

Student absence for religious holidays
A student who intends to observe a religious holy day should make that intention known in writing to the instructor prior to the absence. A student who is absent from classes for the observance of a religious holy day shall be allowed to take an examination or complete an assignment scheduled for that day within a reasonable time after the absence.

Mark Reviewed