STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

American Public University System

The Ultimate Advantage is an Educated Mind

School: Science, Technology, Engineering and Math
Department of Information Technology
Course Number: ISSC266
Course Name: Cryptography Concepts
Credit Hours: 3
Length of Course: 8 Weeks
Prerequisite: None

Table of Contents

Course Description (Catalog)

This course will provide an extensive overview of the field of cryptography, which includes but not limited to a historical perspective on early systems, building to the number theoretic foundations of modern day cryptosystems. Upon completion of this course students will have the ability to demonstrate a knowledge of how cryptosystems are designed, and to match cryptosystems to the needs of an application. Students will also study basic cryptanalysis and will be presented with real life breaches of common cryptosystems so that they better understand the dangers within cryptosystem design and in the design of systems that rely on cryptography. Students will also gain an understanding of the various methods of encryption and analyze the strength and weaknesses of various techniques to ensure data assets are protected and secure.

Table of Contents

Course Scope

This course provides a basic understanding of cryptography in today's world. An explanation of the concepts of cryptography and the historical access of the early cryptographic systems. Information regarding real world breaches of common cryptosystems will also be explored.

Table of Contents

Course Objectives

The successful student will fulfill the following learning objectives:

CO-1: Examine the concepts of cryptography
CO-2: Identify and discuss the different components of Stream and Block Ciphers

CO-3: Analyze Data Encryption Standards (DES) and its alternatives.
CO-4: Analyze and apply the Advanced Encryption Standard (AES) algorithm
CO-5: Identify the types of Public-Key Cryptography
CO-6: Distinguish the structure of RSA and Elliptic Curve Cryptosystems
CO-7: Explain the basic concept of Digital Signatures
CO-8: Examine the concepts of Hash Function and Message Authentication

Table of Contents

Course Delivery Method

This is an eight-week course delivered in the APUS Educator; Distance learning will enable students to complete academic work in a flexible manner, completely online. Resources and access to an online learning management system will be made available to each student. **Online assignments are due by the last day of each week** and include Discussion questions (accomplished in groups through a threaded Discussion), quizzes, and individual assignments (submitted for review by the Faculty Member). Assigned faculty will support the students throughout this eight-week course.

Table of Contents

Course Resources

Additional Resources
See Your Lesson Plan

National Institute of Standards and Technology
Cryptography World
SANS Cyber Security Certifications
Schneier on Security

Table of Contents

Evaluation Procedures

The grading will be based on eight weekly assignments, eight weekly Discussion postings, three weekly quizzes, instructor contacts, and an individual project paper with topic and outline.

1. There will be **eight assignments (5% each) counting a total of 40% of the final grade**. The assignments will follow each of the major milestones of the course. These assignments will be problems or questions from the text. They are a combination of Lesson Reviews and Lesson Activities and/or Labs. They are selected to provide the student with information to understand the concepts discussed. Assignments should be prepared in Microsoft Word using the following file naming convention: ISSC266_Week#Assignment_First_Last.doc(x) (where the # is the week number, and first and last are your first and last names resp.) and submit the file in this assignments' area and uploaded into the student folder by the due date. Any necessary Visio diagrams should be incorporated within the Word document as part of the document.

2. There will be **eight weekly Discussion postings you will need to respond to**. Answers should be 3-4 paragraphs with a **topic sentence** that **restates the question** and **supporting sentences** using the terms, concepts, and theories from the required readings. You may **attack**, **support** or **supplement** other students' answers using the terms, concepts and theories from the required readings. All responses should be a **courteous paragraph** that contains a **topic sentence** with good **supporting sentences**. You may respond multiple times with a continuous discussion with points and counter points. The key requirement is to express your idea and then **support your position** using the terms, concepts and theories from the required readings to demonstrate to me that you understand the material. The Discussion postings will count as 20% (2.5% for each discussion posting) of the final grade.

3. There will be **a project paper (20%)** with **topic selection (1%)**, **outline (2%)** throughout the session, counting as 23% total of the final grade. Please practice using the same file naming convention established in this class for each of these files.

4. There will be quizzes (5% each) a total 15% of the final grade. There will be three non-proctored quizzes. These assessments will cover selected sections of the textbook. It will be a multiple choice and true/false and will be open book and open note
5. Students must make a minimum of 5 classroom Messages (or phone contacts) with the professor beyond the initial contact during the run of the course. Contacts may consist of providing feedback on Resource, questions, comments, related experiences, etc. The Contacts will count as 2% of the final grade.

All assignments, Discussion question responses, and the labs are due by 11:59 Eastern Time Sunday of the week assigned.

GRADING

Grade Instruments	Points Possible	% of Final Grade
Assignment (Weeks 1 to 8)	**700**	**40%**
Discussion Posts (Weeks 1 to 8)	**800**	**20%**
Quizzes (Weeks 3, 5 & 7)	**300**	**15%**
Project Paper Topic (Week 2)	**100**	**1%**
Project Paper Outline (Week 4)	**100**	**2%**
Project Paper Final Product (Week 8)	**100**	**20%**
Contacts (Weeks 1 to 8)	**100**	**2%**
TOTAL	**100 Points**	**100%**

Project Paper (Topic, Outline, PowerPoint Presentation, and Paper) Topics:
Week 2: Topic selection due
Week 4: Outline due
Week 7: Paper due

Topics: Acceptable topics unless I have already approved one:

- Cryptography
- Encryption
- Stream Ciphers
- Block Ciphers
- Public-Key Cryptography
- RSA Cryptosystem
- Digital Signatures
- Elliptic Curve Cryptosystems
- Hash Functions
- Message Authentication Codes
- Key Establishment

Details of Project Paper (20%): You must include at least ten references.
Prepare a 10-15 page paper in Microsoft Word (counts as 20% of the final grade) in APA format (see writing expectations in the Policies section). At a minimum include the following:

- Detailed description of the area researched
- Technology involved in the area
- Future trends in the area

- Example companies involved in the area
- Regulatory issues surrounding the area
- Global implications for the area
- References (minimum of 10)

You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and any other publicly-reviewed source is not accepted). The paper must be at least 10 pages double-spaced, 1" margin all around, black 12 point font (Times New Roman or Arial) with correct citations of all utilized references/sources, (pictures, graphics, etc... are extra - allowed but extra for the minimum page count). The title page and references are also required but don't count in the minimum page count. A minimum of 10 references are required.

The paper will be subjected to checking against plagiarism. The paper must follow acceptable originality criteria (no more than 15% max total, and 2% per individual source match are allowed).

Save the file using the following file naming convention: ISSC366_Project_First_Last.doc(x) (where first and last are your first and last names resp.) and submit the file in this assignment area

Here are the originality report requirements:

1. The originality report must be less than 15% match
2. No single source shall be above 2%
3. You must submit the originality report with your paper to your AMU classroom

If you don't follow these three requirement instructions you will get a 0 for your project paper assignment.
I will give you the chance to rework your papers until an acceptable level of match is achieved.
At the end of the class, if you have not submitted your paper to turnitin.com, I will submit it anyways even after you'd get a 0, to see the level of plagiarism found, if any. If turnitin.com matches more than 40% you will be subject to academic reporting.

8 – Week Course Outline

Please see the Student Handbook to reference the University's grading scale.

Week	Topic	Learning Objectives	Assignment
1	Understanding Cryptography	**CO-1**: Discuss the concepts of cryptography	Week 1 Discussion Week 1 Assignment
2	Symmetrical and Asymmetrical Encryption	**CO-2**: Discuss Symmetrical and Asymmetrical Encryption and other terms like Rounds, Stream and Block Ciphers **CO-3**: Discuss Data Encryption Standards (DES) and its alternatives.	Week 2 Discussion Week 2 Assignment Week 2 Project Paper Topic
3	DES, 3DES and AES	**CO-3**: Discuss Data Encryption Standards (DES) and its alternatives. **CO-4**: Analyze and apply the Advanced Encryption Standard (AES) algorithm	Week 3 Discussion Week 3 Assignment Week 3 Quiz

4	Public-Key RSA and DIFFIE-HELLMAN	**CO-4:** Analyze and apply the Advanced Encryption Standard (AES) algorithm **CO-5:** Compare the types of Public-Key Cryptography **CO-6:** Identify the structure of RSA and Elliptic Curve Cryptosystems	Week 4 Discussion Week 4 Assignment Week 4 Project Paper Outline
5	Hashing and Digital Signatures	**CO-5:** Compare the types of Public-Key Cryptography **CO-6:** Identify the structure of RSA Cryptosystems **CO-7:** Discuss the basic concept of Digital Signatures **CO-8:** Discuss the concepts of Hash Function and Message Authentication	Week 5 Discussion Week 5 Assignment Week 5 Quiz
6	Hash Functions, NON-REPUDIATION and HMAC	**CO-7:** Discuss the basic concept of Digital Signatures **CO-8**: Discuss the concepts of Hash Function, non-repudiation and Message Authentication	Week 6 Discussion Week 6 Assignment
7	Key Establishment	**CO-7:** Discuss the basic concept of Digital Signatures, browser and Server configurations **CO-8**: Discuss the concepts of Hash Function and Message Authentication	Week 7 Discussion Week 7 Assignment Week 7 Quiz
8	Quantum Cryptography		Week 8 Discussion Project Paper with Acceptable Originality Report

Policies

Please see the Student Handbook to reference all University policies. Quick links to frequently asked question about policies are listed below.

Drop/Withdrawal Policy
Extension Process and Policy
Disability Accommodations

Writing Expectations

All written submissions should be submitted in a font and page set-up that is readable and neat. It is recommended that students try to adhere to a consistent format, which is described below.

- Typewritten in double-spaced format with a readable style and font and submitted inside the electronic classroom (unless classroom access is not possible and other arrangements have been approved by the professor).
- Arial 11 or 12-point font or Times New Roman styles.
- Page margins Top, Bottom, Left Side and Right Side = 1 inch, with reasonable accommodation being made for special situations and online submission variances.

Citation and Reference Style

Assignments completed in a narrative essay or composition format must follow APA guidelines. This course will require students to use the citation and reference style established by the American Psychological Association (APA), in which case students should follow the guidelines set forth in *Publication Manual of the American Psychological Association* (6th ed.). (2010). Washington, D.C.: American Psychological Association.

Late Assignments

Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. As adults, students, and working professionals I understand you must manage competing demands on your time. Should you need additional time to complete an assignment please contact me before the due date so we can discuss the situation and determine an acceptable resolution. Routine submission of late assignments is unacceptable and may result in points deducted from your final course grade. Assignments submitted late without a prearranged extension will be subject to a 10% late penalty. **No late assignments will be accepted after the last day of the course.**

Netiquette

Online universities promote the advancement of knowledge through positive and constructive debate – both inside and outside the classroom. Discussions on the Internet, however, can occasionally degenerate into needless insults and "flaming." Such activity and the loss of good manners are not acceptable in a university setting – basic academic rules of good behavior and proper "Netiquette" must persist. Remember that you are in a place for the rewards and excitement of learning which does not include descent to personal attacks or student attempts to stifle the Discussion of others.

- **Humor Note:** Despite the best of intentions, jokes and especially satire can easily get lost or taken seriously. If you feel the need for humor, you may wish to add "emoticons" to help alert your readers: ;-), :), ☺

Disclaimer Statement

Course content may vary from the outline to meet the needs of this particular group.

Online Library

The Online Library is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Online Library provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to **librarian@apus.edu**.

- ***Charles Town Library and Inter Library Loan:*** The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.
- ***Electronic Books:*** You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
- ***Electronic Journals:*** The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.

- ***Tutor*.com**: AMU and APU Civilian & Coast Guard students are eligible for 10 free hours of tutoring provided by APUS. Tutor.com connects you with a professional tutor online 24/7 to provide help with assignments, studying, test prep, resume writing, and more. Tutor.com is tutoring the way it was meant to be. You get expert tutoring whenever you need help, and you work one-to-one with your tutor in your online classroom on your specific problem until it is done.

Request a Library Guide for your course
The AMU/APU Library Guides provide access to collections of trusted sites on the Open Web and licensed resources on the Deep Web. The following are specially tailored for academic research at APUS:

- Program Portals contain topical and methodological resources to help launch general research in the degree program. To locate, search by department name, or navigate by school.
- Course Lib-Guides narrow the focus to relevant resources for the corresponding course. To locate, search by class code (e.g., SOCI111), or class name.

If a guide you need is not available yet, please email the APUS Library: librarian@apus.edu.

Turnitin.com

Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. Typically the course professor will establish a Turnitin.com access code for his/her classes. If the code has not been established, those who wish to use Turnitin.com may ask their professor to establish the code.

Special Note to Faculty: Please be certain to provide accurate directions and to set up the functionality appropriately.

Selected Bibliography