



The University of Texas at El Paso

COURSE NUMBER AND TITLE: ECE 4370/5390 Introduction to Cybersecurity

COURSE DESCRIPTION/COURSE OVERVIEW: Cryptography is an indispensable tool for protecting information in computer systems. In this course you will learn about how cryptographic systems work, and their usage in real-world applications. In this course, students will learn security issues in computer communications, classical cryptographic algorithms, symmetric-key cryptography, public-key cryptography, authentication, and digital signatures. Throughout the course, participants will be exposed to many exciting open problems in the field and work on hands on projects. The lessons are primarily aimed at beginners in this field and hence all the topics are covered in detail (including the theory behind algorithms). As the course progresses more advanced cryptographic tasks, privacy mechanisms, and other forms of encryption and their real time applications would be discussed. These topics should prove useful to those who are new to cybersecurity, and those with some experience.

COURSE TOPICS: This course covers in depth the following key focus areas:

- 1 - Introduction to Cryptography, Core Security Principles, Vulnerabilities and Threats
- 2 - Stream Ciphers, Symmetric-key Crypto
- 3 - DES and Alternatives
- 4 - AES and Block Ciphers
- 6 - Intro to Public-Key Crypto
- 7 - RSA
- 8 - Discrete Logarithm Based Crypto
- 9 - Elliptic Curve Crypto
- 10 - Digital Signatures
- 11 - Hash Functions
- 12 - Considerations while implementing these protocols in real time
- 13 - Key Establishment
- 14 - Privacy Preserving Algorithms and Architectures
- 15 – Applications to Cyber Physical Systems

COURSE PRE-REQUISITES: (1) Students must have successfully completed an undergraduate-level microprocessors course or (2) Topic-wise should understand how a basic computer works, assembly language programming, computer organization.

Prerequisites: *ECE 2304 Microprocessor Systems I* with a grade “C” or better, *MATH 2300 Discrete Mathematics* with a grade “C” or better

COURSE TIME: 1:30 pm to 2:50 pm (Face-to-face)

GENERAL INFORMATION

Dr. Sai Mounika Errapotu

Office Location: Dept of Electrical and Computer Engineering, A-309

Email: serrapotu@utep.edu

Office Hours: Wed 9-10:30 am (in-person or Microsoft Teams)



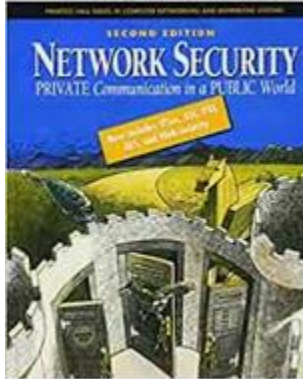
CREDIT ALLOCATION: 3

REQUIRED TEXTBOOKS:

Network Security, Private Communication in a Public World (2nd edition), Pearson Publishers.

ISBN-13: 978-0130460196

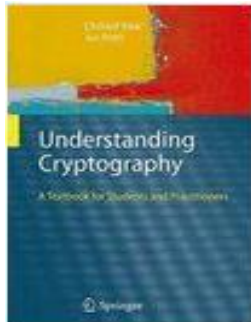
ISBN-10: 0130460192



Understanding Cryptography, Christof Paar and Jan Pelzl

ISBN-13: 978-3642041006

ISBN-10: 3642041000



COURSE OBJECTIVES:

1. **Crypto and Security** - Discuss how cryptography helps to achieve common security goals (data secrecy, message integrity, non-repudiation) and tasks (authentication).
2. **Symmetric vs. Public Key Crypto** - Illustrate the difference between symmetric and public-key cryptography.
3. **Symmetric Crypto** - Explain the notions of symmetric encryption, hash functions, and message authentication, and sketch their formal security definitions.



4. **Symmetric Crypto Practice** - Describe and implement the specifics of some of the prominent techniques for encryption, hashing, and message authentication (e.g, DES, AES, SHA-1, HMAC etc.).
5. **Public Key Encryption** - Explain the notions of public-key encryption and digital signatures, and sketch their formal security definitions. Understanding the mathematical foundations of cryptographic algorithms.
6. **Public Key Crypto Practice** - Describe and implement the specifics of some of the prominent techniques for public-key cryptosystems and digital signature schemes (e.g., RSA, ElGamal, DSA etc.).
7. **Privacy Mechanisms** - Discuss about the role of privacy and its importance in this world of internet. Study algorithms and tools to protect privacy.
8. **Cryptanalysis** - Evaluate cryptographic primitives and their implementations for correctness, efficiency, and security.
9. **Crypto application in modern world:** Study about how cryptography and its application is changing in this inter-connected modern world, strength of security and privacy algorithms.

GRADING POLICY AND STRUCTURE

Time Stamps LMS

- Attendance, participation, and all LMS (Blackboard LMS) postings are counted in Mountain Time (MST). The time stamps in the computer represent MST, regardless of your actual time zone.

Discussion Boards

- Discussion boards will be available if there are any common questions for most of the students in the class.
- Students should follow netiquette rules while participating in discussion boards.

Attendance

- Attendance will be considered from class quizzes (scheduled and surprise quizzes). Students need to participate in the lecture and respond to instructor's questions during the lecture.
- Attendance will be counted in grading.

Assignments

- Assignments are due by **11:59pm (MST)** on the date specified. Assignments **will not be accepted after the due date**. This is done in fairness to those students who turn in their assignments on time. The only exception is with extenuating circumstances or events that have been discussed with the instructor **PRIOR** to the deadline.



Quizzes

- Quizzes will be available for a specific timeframe. There will be **1 attempt** for each quiz for the quizzes posted in blackboard. Only some quizzes have 2 attempts. For quizzes with 2 attempts, the grading criteria varies. Late quizzes will not be accepted. If you would like specific feedback based on your quiz responses, please contact the instructor for an appointment to review your quiz or contact during office hours.

In the case of emergencies when you are prevented from logging on, please contact the Course Faculty as soon as possible by phone and/or email. If you know you will be out of town or otherwise prevented from submitting assignments on the due date, make every effort to turn them in early. Anytime you feel that you are falling behind in the course, it is best to contact the Course Faculty immediately to discuss your situation. In regards to dropping the course with a “W”, it is the **student’s responsibility** to make arrangements with the UTEP Registrar and drop by the “withdrawal date” located on UTEP Registrar website.

Project

- This course constitutes of a final project. You will be working on the project in the second half of the semester. The project grade comprises of the **project idea submission and project review reports (1 and 2)**. Submissions will not be accepted after due date. This is done in fairness to those students who do timely reviews and turn in their reports on time. The only exception is with extenuating circumstances or events that have been discussed with the instructor PRIOR to the deadline.

GRADING SCALE:

Weightage:

5%	Attendance
20%	Quizzes and Discussion Boards
25%	Assignments
25%	Mid Exam
25%	Final Project

Grading scale:

90 - 100	= A
80 - 89	= B
75 - 79	= C
60 - 74	= D
< 60	= F

Assignments, Discussion Boards, Project Reports and Quizzes are always due on Sunday 11:59 pm (MST) *total 100 points*



Expectations of the Class

What should you expect from me as the Lead Faculty?

- I will provide you clear instructions on class expectations
- I will check my **UTEP email/Teams Messages** at least once a day and will get back to you within 24 hours.
- I will timely provide graded feedback on your performance.
- I will keep you informed about your graded progress in the class and will make time to discuss your needs.
- I will leave myself open to suggestions about improvement of the class and class related activities.
- I will do all I can to ensure your learning and success in this class.
- If the course modality needs to be adjusted for any unanticipated reasons, then the class will be notified. If any other changes in the course are to be implemented, I will ensure that the class is notified via announcements in a timely manner.

What Faculty expect of their Students:

- At the beginning of each course, students should review the syllabus and other introductory items located in the **“Week one - Getting started”** folder.
- Students will be expected to complete a **mock assignment and syllabus quiz** on blackboard shell in the first week of class.
- All students are to **review the rules of netiquette and follow in their interaction** with fellow students and faculty for any discussion boards on course topics.
- If the class modality changes to online under any circumstances (like Covid), students need to ensure their internet connection is reliable to timely attend lectures and check class modules.
- If the class mode changes to online under any circumstances, either Blackboard collaborate or MS teams would be used as the medium for course lectures.
- Students are expected to strictly follow the deadlines for quizzes, discussion boards and assignments. Please contact the instructor immediately in case of queries or concerns. If office hours collide with your schedule, email the instructor to schedule alternate time to clarify your queries.

COURSE POLICIES:

Academic Regulations:

Review in UT El Paso Student Handbook the following policies: ***Religious Observance, Ethical and Responsible Use of Social Media, Policy on Academic Integrity, Progression Policy, and Statement on Disability.***

Attendance: Students are expected to attend the class, log-in and check the weekly modules course shell on blackboard (at minimum) **every week** to keep up. Email messages are sent to your **UTEP email address**, so you will want to check your UTEP email everyday as well.



Blackboard:

- Students are required to subscribe to and access the course Blackboard site. Blackboard is the main source of communication between faculty and students. Students are encouraged to access this site daily. Course syllabus, topical outline of scheduled lectures, and assigned readings are posted on this site. Grades of assignments will be made available ONLY through this site.

Communication:

- Communication is the responsibility of both students and faculty. The faculty will keep students informed of progress in theory. Students with questions or concerns should first contact faculty member.
- **Microsoft Teams Online Office Hours, UTEP Email, Teams Messaging** are major technical mediums for interaction. Please feel free to contact the instructor to schedule meetings outside office hours if they collide with your schedule.

Policy on Scholastic Dishonesty:

- Students are expected to be above reproach in all scholastic activities. Students who engage in scholastic dishonesty are subject to disciplinary penalties, including the possibility of failure in the course and dismissal from the College of Engineering and/or university. Scholastic dishonesty includes but is not limited to reproducing test or quiz materials from memory, copy/paste or Xerox, cheating, plagiarism, collusion, the submission for credit or any work or materials that are attributable in whole or in part to another person, taking an examination for another person, and any act designed to give unfair advantage to a student or the attempt to commit such acts. Regents' Rules and Regulations, Part One, Chapter VI, Section 3, Subsection 3.2, Subdivision 3.22.
- Since scholastic dishonesty harms the individual, all students, and the integrity of the College of Engineering and the university, policies on scholastic dishonesty will be strictly enforced. See detailed procedure in the Handbook of Operating Procedures (HOP) available in the Office of the Dean of Students.

Policy relating to Disability / Pregnancy/ CASS:

- Instructor will provide support and help in better understanding the course content, inform the instructor PRIOR to the start of course or during first week of classes to request for additional needs and succeed in the class.
- **Disability:** In Section 504 of the Vocational Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) of 1990, if a student needs an accommodation then the Office of Disabled Student Services located at UTEP need to be contacted. If you have a condition, which may affect your ability to perform successfully in this course, you are encouraged to discuss this in confidence with the instructor and/or the director of the Disabled Student Services. Written guidelines r/t accommodations from CASS must be submitted to the course manager PRIOR to the start of the course. If you have a disability and need classroom accommodations, please contact CASS at 747-5148, or by email to



cass@utep.edu, or visit their office located in UTEP Union East, Room 106. For additional information, please visit the CASS website at www.sa.utep.edu/cass. *CASS' Staff are the only individuals who can validate and if need be, authorize accommodations for students with disabilities.*

- **Pregnancy:** It is the responsibility of the student to inform the instructor of pregnancy limitations. Written guidelines r/t accommodations from The Center for Accommodations and Support Services (CASS) must be submitted to the course manager PRIOR to the start of the course.

Professional Behavior:

- Students are expected to behave professionally *at all times* with faculty, peers, preceptors, and clients **and** in any setting in which the student is a representative of UTEP. Bullying, verbal abuse, insubordination, or personal attacks will not be tolerated in any form. Any behavior deemed inappropriate by faculty and/or preceptors will result in faculty conference(s), and completion of a Student Opting for Success (SOS) plan that addresses the student's areas of needed improvement. Possible activities available to assist the student in attaining the SOS objectives include stress and/or anger management counseling sessions. Inappropriate behaviors may result in an administrative withdrawal from the course and/or dismissal from the program.

Retention: Students Opting for Success (SOS):

- When a student is not progressing in the course as expected, or is not successful on an examination, they will be required to meet with the instructor to discuss strategies for success as outline on the SOS form. The SOS plan will identify recommendations for improving the student's success potential and will specify time lines for completion of these recommendations. The SOS form (with all recommendations completed and all signatures in place) must be submitted to the course manager by due date. *Students who are not successful in the course should be aware that non-compliance with SOS recommendations jeopardizes eligibility for the opportunity to repeat the course in the subsequent semester.* See respective Blackboard home page for SOS form.

Netiquette

"Netiquette" stands for "Internet Etiquette", and refers to the set of practices developed over the years to make the Internet experience pleasant for everyone. Please review some of the **Netiquette** rules.

- At this point in the course, it is also important to share a word of caution, so we can become wiser about interpersonal distance learning communications. As you may know, when communicating electronically, many of the feelings or impressions that are transmitted via body language in face-to-face communications are lost. Consequently, interpreting emotions and innuendoes is far more difficult. Only what is written, or drawn, carries the message. Often excitement can easily be misinterpreted as anger or an insult. It is important that everyone keep this in mind when communicating electronically. Words



in print may appear harmless; however, they can emotionally injure the person reading them. More information can be found at <http://www.albion.com/netiquette>.

Other BB Learn Student Resources

Technical Assistance

This **class** is hosted by UT El Paso. If you have computer, Blackboard problems, or any other kind of technical questions, please contact the UTEP Help Desk via email at helpdesk@utep.edu or by phone at (915) 747-5257. The HELP desk hours are: Mon-Fri 7:00am - 8:00pm (Mountain Time), Sat 9:00am - 1:00pm (Mountain Time), Sun CLOSED.

Copyright Notice

Copyright law protects many of the materials that are posted within this course. These materials are only for the use of students enrolled in this course and only for the purpose of this course. They may not be further retained or disseminated.