COSC 4380 501
Cryptography
Spring 2021 Session 001
Delivery Method: Face to Face

Instructor Information

Name: Sohan Gyawali
Email: gyawali_s@utpb.edu
Phone: 4325522262
Office Location: ST 2264
Office Hours: M, W (2:30 to 4:00 P.M.), T, R (3 to 4:30 P.M.)

Course Information

Class Location: Science & Techn Cntr 1106
Class Time: 05:40 PM

This course covers all the basic and fundamental cryptographic algorithms and security protocols for computer networks such as classical encryptions, DES, AES, RC4, RSA, Diffie-Hellman, ElGamal, Elliptic curve, SHA, MAC etc.

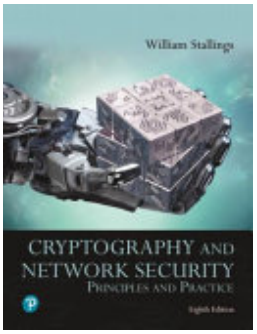
Student Learning Outcomes

- Analyze and design classical encryption techniques and their applications for computer networks.
- Analyze and design block ciphers and their applications for computer networks.
- Understand and analyze data encryption standard.
- Understand and analyze advanced encryption standard.
- Design confidentiality schemes using symmetric encryption.

Sample Syllabus

- Understand and analyze public-key cryptography and RSA.
- Design key management schemes.
- Analyze and design hash and MAC algorithms.
- Analyze and design digital signatures and authentication protocols.

Required Materials



Title: Cryptography and Network Security: Principles and Practice, 8th Edition, William Stallings, Pearson
ISBN: 9780135764268
Authors: William Stallings
Publisher: Pearson
Publication Date: 2019-01-01
Edition: 8th

Important Academic Dates

UTPB Academic Calendar

Graded Material

Grades: Quizzes and Assignments (25 %)

Midterm Exam (25 %)

Final Exam (25 %)

Projects/Labs (25 %)

Bonus (up to 5 %)

Grading Scale

Sample Syllabus

Overall performance of the exams, assignments, and quizzes will determine your final letter grade.

FINAL LETTER GRADE

A = 90% – 100%
B = 80% – 89%
C = 70% – 79%
D = 60% – 69%
F = 0% – 59%

University Policies

Accommodation for Students with Disabilities

Students with Disabilities: The University of Texas Permian Basin in compliance with the Americans with Disabilities Act and Section 504 of the Rehabilitation Act provides "reasonable accommodations" to students with disabilities. Only those students, who an Instructor has received an official Letter of Accommodation (LOA) sent by the Office of ADA for Students, will be provided ADA academic accommodations.

ADA Officer for Students: Mr. Paul Leverington
Address: Mesa Building 4242/4901 E. University, Odessa, Texas 79762
Voice Telephone: 432-552-4696
Email: ada@utpb.edu

For the accessibility and privacy statements of external tools used within courses, go to Accessibility and Privacy Statements.

Sexual Harassment/Sexual Misconduct Policy

The University of Texas Permian Basin (the University) is committed to maintaining a learning and working environment that is free from discrimination based on sex in accordance with Title IX of the Higher Education Amendments of 1972 (Title IX), which prohibits discrimination on the basis of sex in educational programs or activities; Title VII of the Civil Rights Act of 1964 (Title VII), which prohibits sex discrimination in employment; and the Campus Sexual Violence Elimination Act (SaVE Act), Violence Against Women Act (VAWA), and Clery Act.

Sample Syllabus

Sexual Misconduct, Retaliation, and other conduct prohibited under this Policy will not be tolerated and will be subject to disciplinary action.

The University will promptly discipline any individuals or organizations within its control who violate this Policy. The University encourages you to promptly report incidents that could constitute violations of this Policy to the Title IX Coordinator. The complete Sexual Harassment/Sexual Misconduct Policy can be found here.

You may report incidents of sexual misconduct to any University employee. They are obligated to report any incident to the Title IX Coordinator or Deputy Coordinator.

You may also contact:
The UTPB Police Department at 432-552-2786
The Title IX Coordinator at 432-552-2697 or TitleIXCoordinator@UTPB.edu.
The Dean of Students at 432-552-2600
Reports can also be made via the University Complaint Portal: UTPB Complaint Management

A ***confidential reporting option is available***. Please contact UTPB's Counseling Center at 432-552-3365 or 432-552-2367 or stop by MB 1150.

Scholastic Dishonesty

“Scholastic Dishonesty” is any form of cheating or plagiarism that violates the Student Code of Conduct. Scholastic dishonesty or academic dishonesty includes, but is not limited to, cheating, plagiarism, collusion, falsifying academic records, and any act designed to give unfair advantage to the student (such as, but not limited to, submission of essentially the same written assignment for two [2] courses without the prior permission of the instructor, and providing false or misleading information in an effort to receive a postponement or an extension on a test, quiz, or other assignment), or the attempt to commit such an act. The Student Code of Conduct provides students fair notice of conduct considered unacceptable at The University of Texas Permian Basin and which may be the basis for disciplinary action. This policy provides the procedures to be following when student disciplinary action may need to be implemented and outlines the appeals process. The Student Code of Conduct is available online at: https://www.utpb.edu/life-at-utpb/student-services/dean-of-students/student-code-of-conduct

Student Success at UTPB

Sample Syllabus

UT Permian Basin offers numerous services to help you reach your academic goals. Available both in the Success Center on the 2nd Floor of the Mesa Building (https://www.utpb.edu/academics/advising-and-support/student-success-center/index), and online, UTPB Student Success offers the following services to all students:

- O.W .L. (Online Writing Lab) - Submit essays that need to be revised by one of our tutors to owl@utpb.edu.
- Tutoring – For both online and in person tutoring, please use EAB to create an appointment. (Utpb.campus.eab.com) Sign in using UTPB credentials.
- SI/PLTL Sessions - If available for your class, will be communicated to you by the mentor assigned to your class section and students can communicate to their SI or PL through Canvas.
- Peer Mentoring - Incoming freshmen can be paired with a peer mentor who will help you navigate your first year on campus.
- SSC Computer Lab - Come take advantage of the state-of-the-art computers available at the Student Success Center.

Please email success@utpb.edu for more information.

Course Modalities

Both the Texas Higher Education Coordinating Board (THECB) and the Southern Association of Schools and Colleges Commission on Colleges (SACSCOC) provide standard definitions for basic course types/modalities that have informed the following adopted course definitions.

Online Courses are those in which more than 85 percent of the planned instruction occurs online/virtually (asynchronously) when students and faculty are not in the same place. A fully online course is one in which mandatory in-person meetings occur no more than 15% of the planned instructional time.

Remote Courses are ones in which students, while not required to physically come to campus to attend in-person classes, are required to “attend” virtually/remotely (synchronously) during scheduled days and times, with students expected to log in and participate in the lecture via video conferences.

Hybrid Courses are courses in which the majority (more than 50% but less than 85%) of the planned instruction occurs when students and instructor(s) are not in the same place. This form of instruction offers a mix of on-campus/in-person and remote/online/electronic learning.

Sample Syllabus

HyFlex Courses are those which, like hybrid courses, offer a mix of on-campus/in-person and remote/online/electronic learning. These courses, however, do not require student authentication since at least 50% of the planned instruction occurs when students and instructor(s) are in the same place.

Face-to-Face/In-Person Courses are those in which more than 85 percent of the planned instruction occurs when students are in the same place with an instructor(s).

Course Policies

Prerequisite Policy

- Students who are enrolled in the course and have not completed required prerequisites will not be allowed to proceed with a course.
- If students do not have the required prerequisites and do not drop the course voluntarily, they will be dropped administratively.

Attendance Policy

Attendance is **critical**. Students are expected to attend all classes (online as well as face to face). It is your responsibility to obtain any information given out in class. If you miss a class, you are responsible for all course materials presented and for all announcements and/or changes to the syllabus. Some materials presented in the lecture are not covered by the text.

Calculating Attendance:

1. Perfect attendance: gain 3 %
2. Miss 1 class: lose 0 %
3. Miss 2 class: lose 2 %
4. Miss 3 class: lose 3 %
5. Miss 4 class: lose 4 %
6. Miss 5 class: lose 5%

Sample Syllabus

Important: Late arrival or early departure of class meetings is considered as unattended classes unless there are valid excuses in advance.

***Legal Excuses:** Your illness with your doctor's proof. The notified absences with my permission in advance (athletic programs, field trips, etc.). The unexpected events with my permission. Other excuses will not be accepted.

Student Commitment Policy

·Each student is expected to read the text and related materials ***before attending the class.***

- Each student should be prepared to spend an average of at least 8 hours a week outside of class to pass this class.
- Each student should have his/her development environment:
- Example: Computers, Application Programs, Operating Systems, Internet Service Providers (ISP), etc.

Courtesy Policy

Students should be courteous to their instructor and classmates. Any class disturbing behaviors will not be tolerated. No chatting during the class. All phones and pagers must be turned off during the class except an emergency case.

Degrading Policy

Classroom behavior should not interfere with the instructor's ability to conduct the class or the ability of other students to learn from the instructional program (*Code of Student Life*). Unacceptable or disruptive behavior will not be tolerated. Students engaging in unacceptable behavior may be instructed to leave the classroom. Inappropriate behavior may result in disciplinary action or referral to the University's Behavioral Intervention Team.

Sample Syllabus

You will lose 5% of your overall performance if you do the following (each time):

1. Use the computer without instructor's permission.

2. Work on other materials (e.g. other class materials, job related works, internet surfing, etc.) during my class period.

3. Chatting, Eating, and Drinking (Water O.K.).

4. Any class disturbing behaviors.

Cheating Policy

Cheating on exams, quizzes, and all other assignments will not be tolerated. Also, **collaboration and/or plagiarism** are absolutely not tolerated. You must do your own work. ***All like papers will receive the same score – the grade of zero.*** The subject of scholastic dishonesty is addressed more fully in the Student Guide, Appendix B.

Exam and Quiz Policy

- **Quizzes** will be announced or unannounced. There will be **no make-up quizzes without appropriate reasons**. Quizzes will last no longer than 30 minutes. Missed exams or quizzes will be assigned the grade of zero (0).
- **Requests for make-up exams** will be granted under the following conditions:
- There is a very good reason for missing the exam. You are not feeling ready is not an appropriate reason.
- Appropriate reasons for arranging a make-up exam will be accepted by prior arrangement.

Graded Assignments (Exams) Return Policy

Sample Syllabus

- All graded assignments will be given back to the students except the exams. All graded assignments will be passed back to the students during the regular class periods or online. **It is the student's responsibility to receive all graded work at the time that they are passed back.** If a student misses a class on the day a graded assignment is returned, it is the student's responsibility to acquire the graded assignment as soon as possible.
- It is also student's responsibility to resolve all grading problems within one week of the return date of the graded assignment or exam. **No grade will be changed after one week of the return date of the graded assignment or test.**

Assignment Policy

Assignments will be written, programming, or research projects.

- All Assignments are to be submitted by the **end of class or online on the due date.** ***Late assignments will not be accepted unless you get the permission from the instructor. (Please let me know if you have a valid reason and need an extension)***
- First page of your assignment should include your name, course number, section number, and assignment number. No credits will be given for assignment without this information. ***It is required that all assignments returned to students throughout the semester be retained until the end of the semester.***

Format Requirement: The assignment can be handwritten or typed. For each programming assignments, students must submit the code online.

Printing Policy

If the materials are posted on the Web site, it is your responsibility to print all materials from the Web Site before attending the class.

Disclaimer: Instructor reserves the right to modify the policies set forth in this document.

Course Schedule

Sample Syllabus

Week	Topic
1	Syllabus **Chapter 01 - Introduction** What is Network Security? Cryptography? Network Services and Mechanisms, Classification of cryptography techniques
2,3	**Chapter 02 – Classical encryption techniques** Symmetric encryption, Caesar cipher, brute force search, monoalphabetic cipher, playfair cipher, auto key cipher, one time pad, Steganography (1st assignment release (lab))
3	**Chapter 03 – Block cipher** Block cipher, Feistel cipher structure
4,5	**Chapter 04 – DES** DES structure, operation, DES strength, Avalanche effect (2nd assignment release)
5	**Chapter 05 – Number theory**
6	**Chapter 06 – AES** AES structure, AES encryption, AES decryption

Sample Syllabus

	(3rd assignment release)
7	**Chapter 07 - RC4, Block cipher operation**
8	**Review**
9	**Midterm exam**
10	**Chapter 08** – Lecture on OpenSSL (lab), More number theory, (4th assignment release (lab))
11	**Chapter 09** – Public key cryptography and RSA
12	**Chapter 10** – Other public key cryptosystem
13	**Chapter 11** – MAC, Hash functions(5th assignment release)
14	**Chapter 12** – Digital Signature and message authentication
15	Project presentation/demo
16	Final exam review
17	Finals

Sample Syllabus