PRAIRIE VIEW A&M UNIVERSITY

SYLLABUS

COMP 3332 Cryptography
Spring 2024

Course Information	Description
Instructor:	Na Li
Section # and CRN:	P01 23324
Office Location:	S. R. Collins 315
Office Phone:	936-261-9862
Email Address:	nali@pvamu.edu
Office Hours:	MF 10:30am-12pm
Mode of Instruction:	Face to Face
Course Location:	S. R. Collins 226
Class Days & Times:	Tuesday & Thursday 9:30am-10:50am
Catalog Description:	An introduction to the fundamentals of cryptography. It covers various topics, including classic data encryption and decryption schemes, private and public key systems, message authentication, digital signature, and hash function. The course also provides students with hands-on experience in cryptograph.
Prerequisites:	COMP 2310 or COMP 2103 Minimum Grade of C
Co-requisites:	
Required Text(s):	Understanding Cryptography, by Christof Paar and Jan Pelzl, SpringerLink, 2010 (http://crypto-textbook.com)
Recommended Text(s):	Introduction To Modern Cryptography, 2nd Edition Paperback – January 1, 2018 by Yehuda Lindell and Jonathan Katz Publisher : Crc Press (January 1, 2018) ISBN-13 : 978-1138581340 CRC Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press 1996/2001

Course Learning Objectives:

	Upon successful completion of this course, students will be able to:	Student Learning Outcome # Alignment	Core Curriculum Objective Alignment
1	Understand data encryption and decryption schemes	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles	
2	Understand private and public key systems	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles	
3	Understand message authentication	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles	
4	Understand digital signature	Recognize professional responsibilities and make informed judgments in	

		computing practice based on legal and ethical principles	
5	Understand hash function	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles	

Major Course Requirements

Method of Determining Final Course Grade

Course Grade Requirement		Value	Total
1)	Assignments	30%	30%
2)	Mid-term Exam	25%	25%
3)	Final Exam	30%	30%
4)	Presentation	10%	10%
5)	Class Participation	5%	5%
Total:			

Grading Criteria and Conversion:
A = 90% - 100%
B = 80% - 89%
C = 70% - 79%
D = 60% - 69%
F = less than 60%

If a student has stopped attending the course (i.e. “stopped out”) at any point after the first day of class but did not officially withdraw from the course and has missed assignments and exams, including the final exam, and performed below the grade level of a D, a grade of FN (failed-non attendance) will be assigned for the final course grade to ensure compliance with the federal Title IV financial aid regulations. In contrast, if the student has completed all assignments and exams, including the final exam, but performed below the grade level of a D, a grade of F will be assigned for the final course grade.

Detailed Description of Major Assignments:

Assignment Title or Grade Requirement	Description
1. Assignments and Labs	Answer questions about chapters discussed and conduct relevant lab activities
2. Mid-term Exam	Test knowledge learned from chapters
3. Final Exam	Test knowledge learned from chapters
4. Presentations	Relate class learning to real-world cases

Course Procedures or Additional Instructor Policies

Late Assignment Submission

Late assignment submission won’t be accepted.

Missing Exam/Required in-class Activity

If a student misses any exam or required in-class activity, the student must notify the instructor ahead of time. If the reason is university executable, a makeup will be scheduled; otherwise, the student will get zero for the missing exam or activity.

Taskstream
Taskstream is a tool that Prairie View A&M University uses for assessment purposes. One of your assignments may be required to be submitted as an "artifact," an item of coursework that serves as evidence that course objectives are met. If applicable, more information will be provided during the semester, but for general information, you can visit Taskstream via the link in eCourses.

Semester Calendar (tentative schedule)	
Week	**Description**
Week One: **Topic Description**	Introduction to the class; Chapter 1 Introduction to Cryptography
Readings:	
Assignment (s):	
Week Two: **Topic Description**	Chapter 2 Stream Ciphers
Readings:	
Assignment (s):	Assignment 1
Week Three: **Topic Description**	Chapter 3 DES and Alternatives
Readings:	
Assignment (s):	
Week Four: **Topic Description**	Chapter 4 AES
Readings:	
Assignment (s):	Assignment 2
Week Five: **Topic Description**	Chapter 5 More About Block Ciphers
Readings:	
Assignment (s):	
Week Six: **Topic Description**	Chapter 6 Intro to Public-Key Crypto
Readings:	
Assignment (s):	
Week Seven: **Topic Description**	Chapter 7 RSA
Readings:	
Assignment (s):	Assignment 3
Week Eight: **Topic Description**	Mid-Term Exam
Readings:	
Assignment (s):	
Week Nine: **Topic Description**	Spring Break
Readings:	
Assignment (s):	
Week Ten: **Topic Description**	Chapter 8 Discrete Logarithm Based Crypto
Readings:	
Assignment (s):	
Week Eleven: **Topic Description**	Chapter 9 Elliptic Curve Cryptos
Readings:	
Assignment (s):	Assignment 4
Week Twelve: **Topic Description**	Chapter 10 Digital Signatures
Readings:	
Assignment (s):	
Week Thirteen: **Topic Description**	Chapter 11 Hash Functions
Readings:	

Assignment (s):	
Week Fourteen: **Topic Description**	Chapter 12 Message Authentication Codes (MACs)
Readings:	
Assignment (s):	Assignment 5
Week Fifteen: **Topic Description**	Chapter 13 Key Establishment & Presentations
Readings:	
Assignment (s):	
Week Sixteen: **Topic Description**	
Readings:	
Assignment (s):	

Student Support and Success

John B. Coleman Library
The John B. Coleman Library's mission is to enhance the scholarly pursuit of knowledge, to foster intellectual curiosity, and to promote life-long learning and research through our innovative services, resources, and cultural programs, which support the Prairie View A&M University's global mission of teaching, service, and research. It maintains library collections and access both on campus, online, and through local agreements to further the educational goals of students and faculty. Website: https://www.pvamu.edu/library/; Phone: 936-261-1500

Academic Advising Services
Academic Advising Services offers students a variety of services that contributes to student success and leads towards graduation. We assist students with understanding university policies and procedures that affect academic progress. We support the early alert program to help students get connected to success early in the semester. We help refer students to the appropriate academic support services when they are unsure of the best resource for their needs. Faculty advisors support some students in their respective colleges. Your faculty advisor can be identified in PantherTracks. Advisors with Academic Advising Services are available to all students. We are located across campus. Find your advisor's location by academic major at www.pvamu.edu/advising. Phone: 936-261-5911

The University Tutoring Center
The University Tutoring Center (UTC) offers free tutoring and academic support to all registered PVAMU students. The mission of the UTC is to help provide a solid academic foundation that enables students to become confident, capable, independent learners. Competent and caring staff and peer tutors guide students in identifying, acquiring, and enhancing the knowledge, skills, and attitudes needed to reach their desired goals. Tutoring and academic support are offered face-to-face in the UTC, in virtual face-to-face sessions (https://www.pvamu.edu/student-success/sass/university-tutoring-center/), and through online sessions (https://www.pvamu.edu/pvplace/). Other support services available for students include Supplemental Instruction, Study Break, Academic Success Workshops, and Algebra Study Jam. Location: J. B. Coleman Library, Rm. 307; Phone: 936-261-1561; Email: pvtutoring@pvamu.edu; Website: https://www.pvamu.edu/student-success/sass/university-tutoring-center/

Writing Center
The Writing Center provides well-trained peer tutors to assist students with writing assignments at any stage of the writing process. Tutors help students with various writing tasks from understanding assignments, brainstorming, drafting, revising, editing, researching, and integrating sources. Students have free access to Grammarly online writing assistance. Grammarly is an automated proofreading and plagiarism detection tool. Students must register for Grammarly by using their student email address. In addition, students have access to face-to-face and virtual tutoring services either asynchronously via email or synchronously via Zoom. Location: J. B. Coleman Library, Rm. 209; Phone: 936-261-3724; Website: https://www.pvamu.edu/student-success/writing-center/; Grammarly Registration: https://www.grammarly.com/enterprise/signup

Academic Early Alert
Academic Early Alert is a proactive system of communication and collaboration between faculty, academic advisors, and PVAMU students that is designed to support student success by promptly identifying issues and allowing for intervention. Academic Early Alerts help students by providing a central location to schedule advising appointments, view advisor contact information, and request assistance. Students who recognize that they have a problem that is negatively affecting their academic performance or ability to continue school may self-refer an Academic Early Alert. To do so, students will log in to PV Place and click on Academic Early Alert on the left sidebar. Phone: 936-261-5902; Website: https://www.pvamu.edu/student-success/early-alert/

Student Counseling Services
The Student Counseling Services unit offers a range of services and programs to assist students in maximizing their potential for success: short-term individual, couples, and group counseling, as well as crisis intervention, outreach, consultation, and referral services. The staff is licensed by the State of Texas and assists students who are dealing with academic skills concerns, situational crises, adjustment problems, and emotional difficulties. Information shared with the staff is treated confidentially and in accordance with Texas State Law. Location: Hobart Taylor, 2nd floor; Phone: 936-261-3564; Website: https://www.pvamu.edu/healthservices/student-counseling-services/

Office of Testing Services
Testing Services serves to create opportunities by offering a suite of exams that aid in the students' academic and professional success. Currently, we administer entrance (HESI A2), college readiness (TSI assessment), Prior Learning (CLEP, DSST), and proctored exams. Location: Wilhelmina Delco, 3rd Floor, Rm. 305; Phone: 936-261-3627; Email: aetesting@pvamu.edu; Website: www.pvamu.edu/testing

Office of Diagnostic Testing and Disability Services
The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation, contact the Office of Disability Services. As a federally-mandated educational support unit, the Office of Disability Services serves as the repository for confidential disability files for faculty, staff, and students. For persons with a disability, the Office develops individualized ADA letters of request for accommodations. Other services include learning style inventories, awareness workshops, accessibility pathways, webinars, computer laboratory with adapted hard and software, adapted furniture, proctoring non-standardized test administrations, ASL interpreters, ALDs, digital recorders, Livescribe, and a comprehensive referral network across campus and the broader community. Location: Hobart Taylor, Rm. 1D128; Phone: 936-261-3583; Website: https://www.pvamu.edu/disabilityservices/

Center for Instructional Innovation and Technology Services (CIITS)
Distance Learning, also referred to as Distance Education, is the employment of alternative instructional delivery methods to extend programs and services to persons unable to attend college in the traditional manner. The Center for Instructional Innovation and Technology Services (CIITS) supports student learning through online, hybrid, web-assist, and 2-way video course delivery. For more details and contact information, visit:
https://www.pvamu.edu/dlearning/distance-learning-2-2/students-2/; Phone: 936-261-3283

Veteran Affairs
Veterans Services works with student veterans, current military and military dependents to support their transition to the college environment and continued persistence to graduation. The Office coordinates and certifies benefits for both the G.I. Bill and the Texas Hazlewood Act. Location: Evans Hall, Rm. 102; Phone: 936-261-3563; Website: https://www.pvamu.edu/sa/departments/veteranaffairs/

Office for Student Engagement
The Office for Student Engagement delivers comprehensive programs and services designed to meet the co-curricular needs of students. The Office implements inclusive and accessible programs and services that enhance student development through exposure to and participation in diverse and relevant social, cultural, intellectual, recreational, community service, leadership development, and campus governance. Location: Memorial Student Center, Rm. 221; Phone: 936-261-1340; Website: https://www.pvamu.edu/studentengagement/

Career Services
Career Services supports students through professional development, career readiness, and placement and employment assistance. The Office provides one-on-one career coaching, interview preparation, resume and letter writing, and career exploration workshops and seminars. Services are provided for students at the Northwest Houston Center and College of Nursing in the Medical Center twice a month or on a requested basis. Distance Learning students are encouraged to visit the Career Services website for information regarding services provided. Location: Anderson Hall, 2nd floor; Phone: 936-261-3570; Website: https://www.pvamu.edu/careerservices/

University Rules and Procedures

Academic Misconduct
Academic dishonesty is defined as any form of cheating or dishonesty that has the effect or intent of interfering with any academic exercise or fair evaluation of a student's performance. The college faculty can provide additional information, particularly related to a specific course, laboratory, or assignment.

You are expected to practice academic honesty in every aspect of this course and all other courses. Make sure you are familiar with the *University Administrative Guidelines on Academic Integrity*, which can be found on the Academic Integrity webpage. Students who engage in academic misconduct are subject to university disciplinary procedures. As listed in the *University Administrative Guidelines on Academic Integrity*, the University Online Catalog, and the Student Code of Conduct, the following are examples of prohibited conduct. This list is not designed to be all-inclusive

or exhaustive. In addition to academic sanctions, any student found to have committed academic misconduct that is also a violation of criminal law may also be subject to disciplinary review and action by the Office of Student Conduct (as outlined in the Student Code of Conduct).

Forms of Academic Dishonesty:

1. Cheating: Deception in which a student misrepresents that he/she has mastered information on an academic exercise that he/she has not learned, giving or receiving aid unauthorized by the instructor on assignments or examinations. Examples: unauthorized use of notes for a test; using a "cheat sheet" on a quiz or exam; any alteration made on a graded test or exam which is then resubmitted to the teacher;

2. Plagiarism: Careless or deliberate use of the work or the ideas of another; representation of another's work, words, ideas, or data as your own without permission or appropriate acknowledgment. Examples: copying another's paper or answers, failure to identify information or essays from the internet and submitting or representing it as your own; submitting an assignment which has been partially or wholly done by another and claiming it as yours; not properly acknowledging a source which has been summarized or paraphrased in your work; failure to acknowledge the use of another's words with quotation marks;

3. Collusion: When more than one student or person contributes to a piece of work that is submitted as the work of an individual;

4. Conspiracy: Agreeing with one or more persons to commit an act of academic/scholastic dishonesty; and

5. Multiple Submission: Submission of work from one course to satisfy a requirement in another course without explicit permission. Example: using a paper prepared and graded for credit in one course to fulfill a requirement and receive credit in a different course.

Nonacademic Misconduct
The university respects the rights of instructors to teach and students to learn. Maintenance of these rights requires campus conditions that do not impede their exercise. Campus behavior that interferes with either (1) the instructor's ability to conduct the class, (2) the inability of other students to profit from the instructional program, or (3) campus behavior that interferes with the rights of others will not be tolerated. An individual engaging in such disruptive behavior may be subject to disciplinary action. The Office of Student Conduct will adjudicate such incidents under nonacademic procedures.

Sexual Misconduct
Sexual harassment of students and employees at Prairie View A&M University is unacceptable and will not be tolerated. Any member of the university community violating the university's sexual harassment policy will be subject to disciplinary action. In accordance with the Texas A&M University System guidelines, your instructor is obligated to report to the Office of Title IX Compliance (titleixteam@pvamu.edu) any instance of sexual misconduct involving a student, which includes sexual assault, stalking, dating violence, domestic violence, and sexual harassment, about which the instructor becomes aware during this course through writing, discussion, or personal disclosure. The faculty and staff of PVAMU actively strive to provide a learning, working, and living environment that promotes respect that is free from sexual misconduct, discrimination, and all forms of violence. If students, faculty, or staff would like assistance or have questions, they may contact the Title IX Coordinator at 936-261-2144 or titleixteam@pvamu.edu. More information can be found at www.pvamu.edu/titleix, including confidential resources available on campus.

Pregnancy, Pregnancy-related, and Parenting Accommodations
Title IX of the Education Amendments of 1972 prohibits sex discrimination, which includes discrimination based on pregnancy, marital status, or parental status. Students seeking accommodations related to pregnancy, pregnancy-related conditions, or parenting (reasonably immediate postpartum period) are encouraged to contact Student Disability Services or the Dean of Students' Office for additional information and to request accommodations.

Non-Discrimination Statement
Prairie View A&M University does not discriminate on the basis of race, color, sex, religion, national origin, age, disability, genetic information, veteran status, sexual orientation, or gender identity in its programs and activities. The University is committed to supporting students and complying with The Texas A&M University System non-discrimination policy. It seeks to establish an environment that is free of bias, discrimination, and harassment. If you

experience an incident of discrimination or harassment, we encourage you to report it. If you would like to speak with someone who may be able to afford you privacy or confidentiality, there are individuals who can meet with you. The Director of Equal Opportunity & Diversity has been designated to handle inquiries regarding the non-discrimination policies and can be reached at Harrington Science Building, Suite 109 or by phone at 936-261-1744 or 1792.

Class Attendance Policy (See the University Online Catalog for Full Attendance Policy)
Prairie View A&M University requires regular class attendance. Attending all classes supports the full academic development of each learner, whether classes are taught with the instructor physically present or via distance learning technologies such as interactive video and/or the internet. Excessive absenteeism, whether excused or unexcused, may result in a student's course grade being reduced or in the assignment of a grade of "F." Absences are accumulated beginning with the first day of class during regular semesters and summer terms. Each faculty member will include the University's attendance policy in each course syllabus.

Student Academic Appeals Process
Authority and responsibility for assigning grades to students rest with the faculty. However, in those instances where students believe that miscommunication, errors, or unfairness of any kind may have adversely affected the instructor's assessment of their academic performance, the student has a right to appeal by the procedure listed in the University Online Catalog and by doing so within thirty days of receiving the grade or experiencing any other problematic academic event that prompted the complaint.

Technical Considerations

***Minimum* Recommended Hardware and Software:**

- Intel PC or Laptop with Windows 10 or later version; Mac with OS High Sierra*
- Smartphone or iPad/Tablet with Wi-Fi*
- High-speed Internet access
- 8 GB Memory
- Hard drive with 320 GB storage space
- 15" monitor, 800x600, color or 16 bit
- Sound card w/speakers
- Microphone and recording software
- Keyboard & mouse
- Most current version of Google Chrome, Safari, or Firefox

Note: Be sure to enable Java & pop-ups in the Web browser preferences

* Smartphones, Google Chrome books, and Android tablets may not be supported. iPads are the only tablets supported.

Participants should have a basic proficiency of the following computer skills:

- Sending and receiving email
- A working knowledge of the Internet
- Microsoft Word (or a program convertible to Word)
- Acrobat PDF Reader
- Windows or Mac OS
- Video conferencing software

***Netiquette* (online etiquette)**
Students are expected to participate in all discussions and virtual classroom chats as directed. Students are to be respectful and courteous to others on discussion boards. Foul or abusive language will not be tolerated. Do not use ALL CAPS for communicating to others AS IT CAN BE INTERPRETED AS YELLING. Avoid slang terms such as "wassup?" and texting abbreviations such as "u" instead of "you." Limit and possibly avoid the use of emoticons. Be cautious when using humor or sarcasm as tone is sometimes lost in an email or discussion post, and the message might be taken seriously or sound offensive.

Video Conferencing Etiquette
When using Zoom, WebEx, or other video conferencing tools, confirm the visible area is tidy, clear of background clutter, inappropriate or offensive posters, and other distractions. Ensure you dress appropriately and avoid using high traffic or noisy areas. Stay muted when you are not speaking and avoid eating/drinking during the session. Before the class session begins, test audio, video, and lighting to alleviate technology issues.

Technical Support
Students should go to https://mypassword.pvamu.edu/ if they have password issues. The page will provide instructions for resetting passwords and contact information if login issues persist. For other technical questions regarding eCourses, call the Center for Instructional Innovation and Technology Services at 936-261-3283 or email ciits@pvamu.edu.

Communication Expectations and Standards
Emails or discussion postings will receive a response from the instructor, usually in less than 48 hours. Urgent emails should be marked as such. Check regularly for responses.

Discussion Requirement
Online courses often require minimal to no face-to-face meetings. However, conversations about the readings, lectures, materials, and other aspects of the course can occur in a seminar fashion. The use of the discussion board will accomplish this. The instructor will determine the exact use of discussion boards.

It is strongly suggested that students type their discussion postings in a word processing application such as Word and save it to their PC or a removable drive before posting to the discussion board. This is important for two reasons: 1) If for some reason your discussion responses are lost in your online course, you will have another copy; 2) Grammatical errors can be greatly minimized by the use of the spell-and-grammar check functions in word processing applications. Once the post(s) have been typed and corrected in the word processing application, copy and paste to the discussion board.

COVID-19 Campus Safety Measures [NOTE: Delete this section when the COVID-19 pandemic is over]

To promote public safety and protect students, faculty, and staff during the coronavirus pandemic, PVAMU has adopted policies and practices to limit virus transmission.

- **Self-monitoring** - Students should follow CDC recommendations for self-monitoring. Students who have a fever or exhibit symptoms of COVID-19 should participate in class remotely and should not participate in face-to-face instruction.

- **Face Coverings** - Face coverings (cloth face covering, surgical mask, etc.) are recommended in classrooms, teaching laboratories, common spaces such as lobbies and hallways, public study spaces, libraries, academic resource, and support offices, and outdoor spaces where 6 feet of physical distancing is challenging to maintain reliably.

- **Physical Distancing** - Physical distancing should be maintained between students, instructors, and others in course and course-related activities where possible.

- **Personal Illness and Quarantine** - Students required to quarantine are to participate in courses and course-related activities remotely and must not attend face-to-face course activities. Students should notify their instructors of the quarantine requirement. Students under quarantine are expected to participate in courses and complete graded work unless they have symptoms that are too severe to participate in course activities. Students experiencing personal injury or illness that is too severe for the student to attend class qualify for an excused absence. To receive an excused absence, students must provide appropriate documentation to the Office for Student Conduct, studentconduct@pvamu.edu.