



Instructor Information

Instructor: Dr. Robert Jones

Contact: Through Blackboard Ultra or at rtjones@tamu.edu

Class Meeting Time: Thursdays, 1600-1845 (Online Synchronous);

<https://tamusa.zoom.us/j/87017967933?pwd=3tVEkoTMFKv48Ogb4nDe0Uvvuod4w7.1>

Meeting ID 870 1796 7933 / Passcode Fall26~

Office Hours: pop in 30 minutes before each class I teach on Zoom, or by appointment on Zoom when convenient for you; reach out to rtjones@tamu.edu to schedule or for more information or questions.

Course Description

This course covers modern cryptography as it is actually deployed. Students work with symmetric and asymmetric primitives, hash functions, message authentication and authenticated encryption, randomness and CSPRNGs, digital signatures, authentication protocols, and key management, then analyze real protocols for weaknesses and design systems that meet stated security requirements. Coverage extends to cloud key custody, blockchain, post-quantum standards, and the compliance regimes that govern cryptographic deployment.

Credits: 3. This course is about using cryptography correctly. You will implement and break things in a lab, and you will learn why rolling your own primitive is almost always the wrong call. This section is co-taught with CSEC 4380; the two meet together, carry the same requirements, and are graded on the same scale.

Textbook

Optional: Real World Cryptography by David Wong (O'Reilly). Available free to students through the university

O'Reilly subscription: <https://learning.oreilly.com/library/view/real-world-cryptography/9781617296710/>

Everything required to pass this course is provided as OER (Open Educational Resources) in Blackboard or discussed in class. You are never required to buy anything.

Grading Scale

A: 900-1000 B: 800-899 C: 700-799 D: 600-699 F: below 600 points

Course Components

Initial Pretest: 25 points

Assignments (5 x 150 points each): 750 points

Midterm Exam: 75 points

Final Exam: 100 points

Current Events Briefs: 50 points. Domain-specific incidents you find, brief, and assess. Announced in class throughout the semester.

Total: 1000 points.

How Deadlines Work in This Course

Every graded item is assigned in class, and you get a full week minimum. It is due one week later, at 11:59 pm on the night of the class meeting, and I will remind you in class that day. Our class night is Thursday, so that is when things are due. Nothing in this course is ever due on a weekend. If a university holiday falls between the assign date

and the due date, you get the extra week, not less time. The final is the one exception: it lands inside the university final exam window, which can be shorter than a week.

Graded Item	Assigned in class	Due 11:59 pm	Points
Initial Pretest	Thu 8/27 (wk 1)	Thu 9/3	25
Assignment 1	Thu 9/10 (wk 3)	Thu 9/17	150
Assignment 2	Thu 9/24 (wk 5)	Thu 10/1	150
Midterm Exam	Thu 10/8 (wk 7)	Thu 10/15	75
Assignment 3	Thu 10/15 (wk 8)	Thu 10/22	150
Assignment 4	Thu 10/22 (wk 9)	Thu 11/5	150
Assignment 5	Thu 11/5 (wk 11)	Thu 11/19	150
Final Exam	Thu 12/3 (wk 14)	Wed 12/9	100
Current Events Briefs	Throughout the semester	Throughout the semester	50
Optional: Course Evaluation Drop	when course evals open	not graded	drop

Learning Outcomes

By the end of this course, students should be able to:

1. Apply cryptographic algorithms, such as RSA and AES, to secure data and communications, demonstrating proficiency in both their implementation and practical use.
2. Analyze the security of cryptographic protocols, identifying potential vulnerabilities and proposing improvements using formal methods and cryptographic theory.
3. Evaluate the effectiveness of different cryptographic systems in various real-world scenarios, including cloud security and blockchain, by conducting hands-on experiments and case studies.
4. Design a custom cryptographic protocol or secure communication system that meets specific security requirements, incorporating appropriate cryptographic techniques and standards.
5. Demonstrate the ability to solve complex cryptographic problems, such as those involving modular arithmetic, discrete logarithms, or elliptic curves, through both theoretical analysis and practical exercises.

Weekly Schedule (subject to change)

Wk	Date	Topic	Subject Matter
1	8/27/2026	Course Introduction and Cryptography 101	Syllabus overview, threat models, what cryptography does and does not solve
2	9/3/2026	Symmetric Key Cryptography	Block and stream ciphers, AES, modes of operation, padding
3	9/10/2026	Asymmetric Key Cryptography	RSA, Diffie-Hellman, elliptic curves, key sizing
4	9/17/2026	Hash Functions, MACs, and Authenticated Encryption	Collision resistance, HMAC, GCM, ChaCha20-Poly1305, AEAD
5	9/24/2026	Randomness, Entropy, and CSPRNGs	Entropy sources, seeding, PRNG failure modes and real-world breaks
6	10/1/2026	Key Management and Distribution	Key lifecycle, PKI, certificate validation, hardware security modules
7	10/8/2026	Cryptographic Attacks	Padding oracles, timing and side channels, nonce reuse, downgrade attacks
8	10/15/2026	Digital Signatures and Authentication Protocols	Signature schemes, Kerberos, the TLS handshake, mutual authentication
9	10/22/2026	Applied Cryptography in Secure Communications	TLS in practice, messaging protocols, forward secrecy
10	10/29/2026	Blockchain and Cryptography	Consensus, digital signatures at scale, wallet key handling
11	11/5/2026	Post-Quantum Cryptography	Shor and Grover, ML-KEM, ML-DSA, SLH-DSA, FIPS 203/204/205, hybrid TLS migration
12	11/12/2026	Protocol Design and Analysis	Building to stated requirements, formal reasoning, failure modes

Wk	Date	Topic	Subject Matter
13	11/19/2026	Cryptography in the Cloud and Keeping Privacy Alive	Key custody, envelope encryption, confidential computing, metadata exposure
	11/26/2026	No Class. Thanksgiving Holiday, University Closed	N/A
14	12/3/2026	Cryptographic Standards and Compliance	FIPS, NIST guidance, audit evidence, course wrap-up
	12/5-12/11	Final Exam Week. No class meeting	Final Exam submitted in Blackboard

Important Fall 2026 Dates

Date	Event
August 24	First day of class
September 4	Deadline to notify instructor of religious observances (end of second week)
September 7	Labor Day Holiday. No classes, University closed
September 9	Census Date. Students not paid in full or enrolled in a payment plan by 4:59 pm may be dropped for non-payment
October 5 to October 16	Midterm grading period
November 13	Last day to drop with an automatic W
November 25	Study Day. No classes
November 26 to November 28	Thanksgiving Holiday. No classes, University closed
November 30	Last day to drop a course or withdraw from the University
December 4	Last day of classes
December 5 to December 11	Final exams
December 15	Commencement

The complete Academic Calendar is available on our website.

Course Policies

Weekly Assignment Availability and Due Dates: You will receive a minimum of 1 week to complete all assignments. All assignments will be submitted in Blackboard. Due dates for assignments will be clearly indicated in Blackboard. Assignments, unless noted, should be submitted as ONE DOCUMENT in docx/pdf format unless otherwise noted.

Deadline/Late Policy: This assignment is to be completed and submitted through Blackboard no later than the deadline/due-date indicated on the Blackboard. Contact Dr. Jones immediately using the Blackboard Inbox or by email if you require any assistance. If for technical or personal reasons, you miss the deadline/due date, you may submit the assignment up until, but no later than, the late submission window.

Assignments are not accepted for any reason after the late submission window and there are no makeup assignments. Missing assignments are recorded as a zero grade. If you miss the due date, even by a minute for technical or personal reasons you are late. Send your Instructor a message through Blackboard Inbox on or before the due/deadline if you need to get assistance so there is time to respond and for you to take the appropriate actions to complete and submit the assignment. Students are expected to continue to work diligently to complete any assignment while in communication with Dr. Jones. Late work will be penalized 10% per day and will not be accepted after 5 days.

If you miss more than 2 total assignment due dates entirely without contacting the instructor prior to the closing of the late window for the second assignment, the instructor reserves the right (and will probably start the process) to drop you from the course.

When Work Will be Graded: Work will be graded within 1 week after it is due and most students have completed the assignment. Even if you turn in something the day it is assigned, do not expect a grade before the assignment is

actually due. During certain circumstances such as midterm grade posting or other similar events, the instructor may grade work ahead of this schedule to improve student visibility to grades during key periods.

Grades: Check your Grades often in Blackboard. Each student is expected to review his or her graded assignments promptly each week. Changes to a student's grade will only be made upon request made through Blackboard Inbox within 1 week after an assignment is graded, and only if the individual student provides clear evidence that is accepted by the Instructor as to why their answer should be accepted and the grade changed. Discussing grades or other academic concerns on discussion boards or group messages in this course is not permitted.

Drop Grade for Course Evaluation: If you complete a course evaluation in the class you may drop any one assignment, past or future, from the course. The total amount of points that you will be graded on changes from 1000 to whatever is left, and your grade will be calculated based on the percentage of points you have compared to your revised, lower total after a grade drop. You may initiate this grade drop when the course evaluation period opens and the instructor posts a special 0 point assignment.

Incomplete Grades: There are very few situations in which I will ever consider giving out an incomplete grade. One exception is military deployment and another is life threatening illness. You must be passing at the time of requesting an incomplete grade. If you feel that your situation warrants this consideration, contact me as soon as possible.

Student responsibility to contact instructor: There is always a lot going on in the world and I am here to help you, but please help me help you! Keep me posted if you need additional assistance, resources, or have something going on that will factor into you being successful in this class. I would rather hear from you more often than not often enough.

Final Exam Format: This course is delivered online synchronous. There is no live final exam meeting. The final opens at our last class on 12/3 and is submitted in Blackboard by 11:59 pm on Wednesday 12/9, inside the university final exam window of December 5 through December 11. It is not due on a weekend.

Artificial Intelligence Policy

Insert ONE of the AI policy options listed below in your syllabi. Select the one you believe is most appropriate for your course.

Option 1 - No Use of Generative AI Permitted

[Insert Course Number] assumes that all work submitted by students will be generated by the students themselves, working individually or in groups. Students should not have another person/entity do the writing of any portion of an assignment for them, which includes hiring a person or a company to write assignments and/or using artificial intelligence (AI) tools like ChatGPT. Use of any AI-generated content in this course qualifies as academic dishonesty and violates Texas A&M-San Antonio's standards of academic integrity.

Option 2 - Use of Generative AI Permitted Under Some Circumstances or With Explicit Permission

There are situations and contexts within this course where you may be asked to use artificial intelligence (AI) tools to explore how they can be used. Outside of those circumstances, you should not use AI tools to generate content (text, video, audio, images) that will end up in any student work (assignments, activities, discussion responses, etc.) that is part of your evaluation in this course. Any student work submitted using AI tools should clearly indicate with attribution what work is the student's work and what part is generated by the AI. In such cases, no more than 25% of the student work should be generated by AI. If any part of this is confusing or uncertain, students should reach out to their instructor for clarification before submitting work for grading. Use of AI-generated content without the instructor's permission and/or proper attribution in this course qualifies as academic dishonesty and violates Texas A&M-San Antonio's standards of academic integrity.

Option 3 - Broader Use of Generative AI Permitted Within Guidelines

Use of artificial intelligence (AI) tools, including ChatGPT, is permitted in this course for students who wish to use them. To adhere to our scholarly values, students must cite any AI-generated material that informed their work (this includes in-text citations and/or use of quotations, and in your reference list). Using an AI tool to generate content without proper attribution qualifies as academic dishonesty and violates Texas A&M-San Antonio's standards of academic integrity.

Option 4 - Customized Policy Generative AI Policy

Faculty may create a customized policy that is unique for a specific course with consultation from the department chair. Faculty are encouraged to view Texas A&M University's Generative AI Syllabus Statement Considerations when preparing a customized AI policy.

NOTE: Guidance for how to cite AI-generators, like ChatGPT, can be found here
<https://apastyle.apa.org/blog/how-to-cite-chatgpt>

Oh, he picks 3 for AI. I left all four in on purpose, along with the bracket where I was supposed to type my own course number. Read them. Then notice that the university handed me four options and

told me to pick one, and that the pick changes what counts as cheating in this room. Rules are written by people, they get pasted around, and sometimes the paste is the whole story. Follow them to the letter. Then ask whether they make sense. Knowing when a rule bends and when it breaks is the actual job.

University Wide Stuff and No, I Don't Know Why They Used Blue Font

University Email Policy and Course Communications

All correspondence between professors and students must occur via university email accounts. You must have your Jaguar email account ready and working. If it is not working, contact the help desk at helpdesk@tamusa.edu or at 210-784-HELP (4357). If you don't hear back within 48 hours, contact them again. They have many requests during the first part of the semester, so you may need to follow up with them.

Academic Accommodations for Individuals with Disabilities

Texas A&M University-San Antonio is committed to providing all students with reasonable access to learning opportunities and accommodations in accordance with The Americans with Disabilities Act, as amended, and Section 504 of the Rehabilitation Act. If you experience barriers to your education due to a disability or think you may have a disability, Disability Support Services is located in the Central Academic Building, Suite 210. You can also contact us via phone at (210) 784-1335, visit us at the website or email us at dss@tamusa.edu. All students are encouraged to discuss their academic accommodation with Disability Support Services and their instructors as soon as possible.

Academic Learning Center

All currently enrolled students at Texas A&M University-San Antonio can utilize the Academic Learning Center for subject-area tutoring. The Academic Learning Center provides free course-based tutoring to all currently enrolled students. Students wishing to work with a tutor can make appointments through the Brainfuse online tutoring platform. Brainfuse can be accessed in the Tools section of Blackboard. You can contact the Academic Learning Center by emailing tutoring@tamusa.edu, calling (210) 784-1307, or visiting the Central Academic Building, room 202. Online tutoring is also available for after hours and weekend assistance.

While tutoring hours may change based on tutor schedules and availability, the current tutoring hours for MATH in the ALC are as follows:

Day	Appointments available	Walk in Tutoring, no appointment needed
MONDAY	8 am to 6 pm	9 am to 5 pm
TUESDAY	8 am to 6 pm	9 am to 5 pm
WEDNESDAY	8 am to 6 pm	9 am to 5 pm
THURSDAY	8 am to 6 pm	9 am to 5 pm
FRIDAY	8 am to 5 pm	11 am to 4 pm

Counseling/Mental Health Resources

As a college student, there may be times when personal stressors interfere with your academic performance and negatively impact your daily functioning. If you are experiencing emotional difficulties or mental health concerns, support is available to you through the Student Counseling Center (SCC). To schedule an appointment, visit our website, call 210-784-1331 or visit Madla 120 between the hours of 8:00 AM and 5:00 PM.

All mental health services provided by the SCC are free and confidential (as the law allows). The Student Counseling Center provides brief individual and group therapy, crisis intervention, consultation, case management, and prevention services. Crisis support is available 24/7/365 by calling the SCC at 210-784-1331 or through the TELUS student support App.

The TELUS Student Support App provides a variety of mental health resources including 24/7/365 support for in the moment distress, crisis support, an anonymous peer-to-peer support network, mental health screenings, podcasts, and articles to improve your mental wellbeing.

[A qr code on a white background]

Emergency Preparedness

JagE Alert is Texas A&M University-San Antonio's mass notification system. In the event of an emergency, such as inclement weather, students, staff and faculty, who are registered, will have the option to receive a text message or email with instructions and updates. To register or update your information visit: <https://tamusa.bbcportal.com/>. More information on emergency response may be found in the Emergency Operations Plan and the Emergency Action Plan. Download the SafeZone App (<https://safezoneapp.com/>) for emergencies or call (210) 784-1911. Non-Emergency (210) 784-1900.

Financial Aid and Verification of Attendance

According to federal regulation 34 CFR 668.21, a student can only receive Title IV funds based on Title IV eligibility criteria which include class attendance. If Title IV funds are disbursed to ineligible students (including students who fail to begin attendance), the institution must return these funds to the U.S. Department of Education within 30 days of becoming aware that the student will not or has not begun attendance. Faculty will provide the Office of Financial Aid with an electronic notification if a student has not attended by the published Census Date (the first week of class). Any student receiving federal financial aid who does not attend prior to the published Census Date will have their aid terminated and returned to the DoE. Please note that any student who stops attending at any time during the semester may also need to return a portion of their federal aid.

Jaguar Writing, Language, and Digital Composing Center (WLDCC)

The WLDCC provides support to graduate and undergraduate students in all three colleges as well as faculty and staff. Writing tutors work with students to develop reading skills, prepare oral presentations, and plan, draft, and revise their written assignments. Our language tutors support students enrolled in Spanish courses and students composing in Spanish for any assignment. Our digital studio tutors support

students working on digital projects such as eportfolios, class presentations, or other digital multimedia projects. The WLDCC offers face-to-face, synchronous online, and asynchronous digital appointments. Students can schedule appointments with the WLDCC in JagWire under the Student Services tab. The WLDCC can also be reached by emailing wldcc@tamusa.edu.

Meeting Basic Needs

Any student who has difficulty affording groceries or accessing sufficient food to eat every day or who lacks a safe and stable place to live, and believes this may affect their performance in the course, is urged to submit a CARE report for support. Furthermore, please notify the professor if you are comfortable in doing so. This will enable them to direct you to available resources. A food pantry is available on campus.

Military Affairs

Veterans and active-duty military personnel are welcomed and encouraged to visit the Office of Military Affairs for any question involving federal or state VA Education Benefits. Visit the Patriots' Casa building, room 202, or contact the Office of Military Affairs at military.va@tamusa.edu or (210) 784-1397.

Religious Observances

Texas A&M University-San Antonio recognizes the wide variety of faiths represented among the campus community and protects the rights of students, faculty, and staff to observe religious holidays according to their tradition. Under the policy, students are provided an opportunity to make up any examination, study, or course work requirements that may be missed due to a religious observance provided they notify their instructors before the end of the second week of classes for regular session classes.

The Six-Drop Rule

Students are subject to the requirements of Senate Bill (SB) 1231 passed by the Texas Legislature in 2007. SB 1231 limits students to a maximum of six (6) non-punitive course drops (i.e., courses a student chooses to drop) during their undergraduate careers. A non-punitive drop does not affect the student's GPA. However, course drops that exceed the maximum allowed by SB 1231 will be treated as F grades and will impact the student's GPA.

Statement of Harassment and Discrimination

Texas A&M University-San Antonio is committed to the fundamental principles of academic freedom, equal opportunity, and human dignity. To fulfill its multiple missions as an institution of higher learning, A&M-San Antonio encourages a climate that values and nurtures collegiality and the uniqueness of the individual on our campus and within our state, nation, and world. All decisions and actions involving students and employees are to be based on applicable law and individual merit. Texas A&M University-San Antonio, in accordance with applicable federal and state law, prohibits discrimination, including harassment, on the basis of race, color, sex, religion, national origin, age, disability, genetic information, veteran status, sexual orientation, or pregnancy/parenting status. Individuals who believe they have

experienced harassment or discrimination prohibited by this statement are encouraged to contact the University's Civil Rights Officer at 210-784-2061 or titleix@tamusa.edu.

Texas A&M University-San Antonio faculty are committed to providing a safe learning environment for all students and for the university as a whole. If you have experienced any form of sex discrimination or harassment, including sexual assault, sexual harassment, domestic or dating violence, or stalking based on sex, know that help and support are available. A&M-San Antonio's Title IX Coordinator can support those impacted by such conduct in navigating campus life, accessing health and counseling services, providing academic and housing accommodations, and more. The university strongly encourages all students to report any such incidents to the Title IX Coordinator. Please be aware that all A&M-San Antonio employees (other than those designated as confidential resources such as counselors and trained victim advocates) are required to report information about such discrimination and harassment to the university. This means that if you tell a faculty member about a situation of sexual harassment, sexual violence, or other related sex-based misconduct, the faculty member must share that information with the university's Title IX Coordinator (titleix@tamusa.edu, 210-784-2061, CAB 439K). If you wish to speak to a confidential employee who does not have this reporting requirement, you can contact the Student Counseling Center at (210) 784-1331 or visit them in Madla 120.

Pregnant/Parenting Students

Texas A&M-San Antonio does not require a pregnant or parenting student, solely because of that status or issues related to that status, to (1) take a leave of absence or withdraw from their degree or certificate program; (2) limit the student's studies; (3) participate in an alternative program; (4) change the student's major, degree, or certificate program; or (5) refrain from joining or cease participating in any course, activity, or program at the University. The university will provide such reasonable accommodations to pregnant students as would be provided to a student with a temporary medical condition that are related to the health and safety of the student and the student's unborn child. Pregnant/parenting students are encouraged to contact the Title IX Coordinator with any questions or concerns related to their status (titleix@tamusa.edu; 210-784-2061; CAB 439K).

Texas A&M-San Antonio has also designated the Title IX Coordinator as the liaison officer for current or incoming students who are the parent or guardian of a child younger than 18 years of age. Young Jaguars can support parenting students with daycare if students meet this criteria: (1) must be enrolled in classes at Texas A&M-San Antonio in the current semester, (2) must be Pell eligible or a single parent, (3) child(ren) must be aged 3 to 12-years-old, and (4) child(ren) must be enrolled in Pre-K-3 through 6th grade. Hours of operation are Monday-Thursday 3:30pm-9:00pm. For more information, please contact Young Jaguars at youngjaguars@tamusa.edu or call (210) 784-2636.

Students' Rights and Responsibilities

The following statement of students' rights and responsibilities is intended to reflect the philosophical base upon which University Student Rules are built. This philosophy acknowledges the existence of both rights and responsibilities, which is inherent to an individual not only as a student at Texas A&M University-San Antonio but also as a citizen of this country.

Students' Rights

1. A student shall have the right to participate in a free exchange of ideas, and there shall be no University rule or administrative rule that in any way abridges the rights of freedom of speech, expression, petition and peaceful assembly as set forth in the U.S. Constitution.
2. Each student shall have the right to participate in all areas and activities of the University, free from any form of discrimination, including harassment, on the basis of race, color, national or ethnic origin, religion, sex, disability, age, and pregnancy/parenting or veteran status in accordance with applicable federal and state laws.
3. A student has the right to personal privacy except as otherwise provided by law, and this will be observed by students and University authorities alike.
4. Each student subject to disciplinary action arising from violations of university student rules shall be assured a fundamentally fair process.

Students' Responsibilities

1. A student has the responsibility to respect the rights and property of others, including other students, the faculty, and administration.
2. A student has the responsibility to be fully acquainted with the published University Student Rules found in the Student Handbook, Student Code of Conduct, on our website, and University Catalog, and to comply with them, as well as with federal, state, and local laws.
3. A student has the responsibility to recognize that student actions reflect upon the individuals involved and upon the entire University community.
4. A student has the responsibility to recognize the University's obligation to provide a safe environment for learning.
5. A student has the responsibility to check their university email for any updates or official university notifications.

We expect that students will behave in a manner that is dignified, respectful, and courteous to all people, regardless of sex, ethnic/racial origin, religious background, or disability. Conduct that infringes on the rights of another individual will not be tolerated.

Students are expected to exhibit a high level of honesty and integrity in their pursuit of higher education. Students engaging in an act that violates the standards of academic integrity will find themselves facing academic and/or disciplinary sanctions. Academic misconduct is any act, or attempt, which gives an unfair advantage to the student. Additionally, any behavior specifically prohibited by a faculty member in the course syllabus or class discussion may be considered as academic misconduct. For more information on academic misconduct policies and procedures please review the Student Code of Conduct or visit the resources available in the OSRR website.