Welcome to Cryptography! *The following quote frames your study in this course.*

"The world doesn't care what you know. The world cares what you can do with what you know." (Wagner and Compton 2015)

In this course, as in all of my courses, I aim to help my students develop a combination of technical knowledge and workplace skills that the job market values, consistent with the above quote.

The Voice of the Market—Please consider the following excerpt from one of my students from the spring of 2019:

> I just wanted to shoot you a quick email to thank you for what you've taught me.
>
> I got a job at XXX, a multi-billion-dollar consulting company. They just opened this office eighteen months ago and are establishing their cybersecurity headquarters for the whole USA in this office. It's a huge room, still under construction, with multiple security measures (separate key cards, bio metric scanning, etc.) They're looking to staff more people in it and it's where I'll be working once I complete training.
>
> As you can imagine, the training is very rigorous. Classroom sessions, exams where anything under a 100 is failing, the whole nine yards. EVERYTHING you've mentioned about cybersecurity has been covered and emphasized. I've been able to retain information and apply it in practice because of the way you taught it to me. When one of the instructors asked me how I knew certain things or am familiar with certain practices, I answered, "Dr. Hull taught me."
>
> Whatever research you have going on in regards to behavioral cybersecurity, please continue. There's a lot of anxiety in being part of a team that protects billions of dollars' worth of assets, but you're teaching has definitely helped me. I'm sure there's many more prospective security analysts who would also benefit under your guidance.

***Course Description*:** COSC 5367/4367 provides an overview to cryptography, which includes classical encryption, block ciphers and DES, public key cryptography, hashing, message authentication, key management, digital signatures, user authentication, transport layer security, wireless security, and e-mail security.

Revisions to the Syllabus—*The instructor may revise the syllabus where necessary to achieve the course learning outcomes.*

Course Learning Outcomes: Upon completion of this course, students should know and be able to apply:

- The fundamental concepts and principles of computer security
- The principles of symmetric ciphers
- The principles of asymmetric ciphers

- The principles of cryptographic data integrity algorithms
- The principles of mutual trust
- The fundamental concepts and principles of network security

Prerequisite: COSC 4325 or COSC 4360 or equivalent.

Required Textbook: None

Class Time—MWF 10:10 to 11:05 – COB 211 See Appendix A regarding hybrid-course structure, which we will follow if our delivery format changes from in-classroom delivery to online delivery. See Appendix B regarding guidance for COVID-related matters.

Instructor Information—Dr. David Michael Hull, Assistant Professor, Computer Science Dept., COB 315.06. dhul@uttyler.edu

Office Hours—M/W/F 11:15 – 12:15.

Table 2. Schedule of Modules and Their Content Coverage

Module #	Chapter	Topics
1	1, 3	Course overview; Computer and Network Security Concepts; Classic Encryption Techniques
2	4,6	Block Ciphers and the Data Encryption Standard (DES) and Advanced Encryption Standard (AES)
3 & 4	9, 10, 11	Public-Key Cryptography and RSA; Other Public-key Cryptosystems; Cryptographic Hash Function
5	Essay Exam # 1—Monday (take exam) and Friday (review exam) Wednesday—Security in the age of the Internet of Things: Profound Career Implications[1]	
6	12, 13	Message Authentication; Digital Signatures
7 & 8	14, 15	Key Management and Distribution; User Authentication
9	16, 17	Network Access Control and Cloud Security; Transport-Level Security
10	Essay Exam # 2—Monday (take exam) and Friday (review exam) Wednesday—The Weaponization of Encryption[2]	
11 & 12	18, 19, 20	Wireless Network Security; Email Security; IP Security
13, 14	Comprehensive Semester-end Projects: Presentations, Feedback and Reflection Activities	

Notice that in each module, we will cover two or three chapters of content. That's a lot of reading, especially given that the content

[1] This topic is explored in Bauer et al. (2017).
[2] This topic is explored in ArborNetworksEditors (2017).

Grading Rubric:

Letter Grade	Assigned Score (s)			Definition
A	90 %	≤ s		Mastery
B	80 %	≤ s <	90 %	Good Understanding
C	70 %	≤ s <	80 %	Adequate
D	65 %	≤ s <	70 %	Probably Failed to Demonstrate
F		s <	65 %	Definitely Failed to Demonstrate

Exams: Tests must be taken when scheduled. No makeup tests or exams will be given. The instructor may make exceptions in extreme cases.

Expectations of students:

- **Take ownership of your learning.** You are responsible for what you get out of this course. I have organized the course to emphasize two goals: The acquisition of relevant knowledge and the development of the skillful use of that knowledge. In Week 1, we will review and discuss the rationale for this method of promoting deep learning.
- **Team-Based Learning.** Notice that a substantial portion of your grade is associated with the team-based learning activities. Such activities are vital to helping you learn how to skillfully apply acquired knowledge.
- **Essay Exams.** Notice that the exams are essay-based. This form of exam promotes and measures the reasoning and communication skills you need to skillfully apply acquired knowledge in the real world.
- **Importance of Attending Class**—As detailed in the Course Overview document, we will follow the "flipped classroom" model whereby we devote much of our classroom time not to lecture but instead to experiential learning exercises that help you develop your ability to apply relevant knowledge, using effective communication skills, teamwork skills and problem-solving skills. Thus, attending class is vitally important to your learning and academic performance.

University Policies

The following pages may be revised without notice. These policies can be found on UT Tyler's website: http://www.uttyler.edu/academicaffairs/files/syllabuspolicy.pdf

UT Tyler Honor Code – Every member of the UT Tyler community joins together to embrace: Honor and integrity that will not allow me to lie, cheat, or steal, nor to accept the actions of those who do.

Student Standards of Academic Conduct – Disciplinary proceedings may be initiated against any student who engages in scholastic dishonesty, including, but not limited to, cheating, plagiarism, collusion, the submission for credit of any work or materials that are attributable in whole or in part to another person, taking an examination for another person, any act designed to give unfair advantage to a student or the attempt to commit such acts.

"Cheating" includes, but is not limited to:

- copying from another student's test paper or homework assignment;
- using, during a test, materials not authorized by the person giving the test;
- failure to comply with instructions given by the person administering the test;
- possession during a test of materials which are not authorized by the person giving the test, such as class notes or specifically designed "crib notes". The presence of textbooks constitutes a violation if they have been specifically prohibited by the person administering the test;
- using, buying, stealing, transporting, or soliciting in whole or part the contents of an unadministered test, test key, homework solution, or computer program;
- collaborating with or seeking aid from another student during a test or other assignment without authority;
- discussing the contents of an examination with another student who will take the examination;
- divulging the contents of an examination, for the purpose of preserving questions for use by another, when the instructors has designated that the examination is not to be removed from the examination room or not to be returned or to be kept by the student;
- substituting for another person, or permitting another person to substitute for oneself to take a course, a test, or any course-related assignment;
- paying or offering money or other valuable thing to, or coercing another person to obtain an unadministered test, test key, homework solution, or computer program or information about an unadministered test, test key, home solution or computer program;
- falsifying any academic work offered for credit;
- taking, keeping, misplacing, or damaging the property of The University of Texas at Tyler, or of another person, if the student knows or reasonably should know that an unfair academic advantage would be gained by such conduct; and
- misrepresenting facts, including providing false grades or resumes, for the purpose of obtaining an academic or financial benefit or injuring another student academically or financially.

Unless otherwise specified, all work submitted for a grade must be work that you completed alone. You are not to submit another person's work and claim it as your own. Plagiarism and/or collusion will result in disciplinary actions.

Students Rights and Responsibilities – To know and understand the policies that affect your rights and responsibilities as a student at UT Tyler, please follow this link:

http://www.uttyler.edu/wellness/rightsresponsibilities.php

Grade Replacement/Forgiveness and Census Date Policies – Students repeating a course for grade forgiveness (grade replacement) must file a Grade Replacement Contract with the Enrollment Services Center (ADM 230) on or before the Census Date of the semester in which the course will be repeated. (For Fall, the Census Date is Sept. 10.) Grade Replacement Contracts are available in the Enrollment Services Center or at http://www.uttyler.edu/registrar. Each semester's Census Date can be found on the Contract itself, on the Academic Calendar, or

in the information pamphlets published each semester by the Office of the Registrar. Failure to file a Grade Replacement Contract will result in both the original and repeated grade being used to calculate your overall grade point average. Undergraduates are eligible to exercise grade replacement for only three course repeats during their career at UT Tyler; graduates are eligible for two grade replacements. Full policy details are printed on each Grade Replacement Contract. The Census Date (Sept. 10th) is the deadline for many forms and enrollment actions of which students need to be aware. These include:

- Submitting Grade Replacement Contracts, Transient Forms, requests to withhold directory information, approvals for taking courses as Audit, Pass/Fail or Credit/No Credit.
- Receiving 100% refunds for partial withdrawals. (There is no refund for these after the Census Date)
- Schedule adjustments (section changes, adding a new class, dropping without a "W" grade)
- Being reinstated or re-enrolled in classes after being dropped for non-payment
- Completing the process for tuition exemptions or waivers through Financial Aid

State-Mandated Course Drop Policy – Texas law prohibits a student who began college for the first time in Fall 2007 or thereafter from dropping more than six courses during their entire undergraduate career. This includes courses dropped at another 2-year or 4-year Texas public college or university. For purposes of this rule, a dropped course is any course that is dropped after the census date (See Academic Calendar for the specific date). Exceptions to the 6-drop rule may be found in the catalog. Petitions for exemptions must be submitted to the Enrollment Services Center and must be accompanied by documentation of the extenuating circumstance. Please contact the Enrollment Services Center if you have any questions.

Last Day to Withdraw—From the first day of classes through the Last Day to Withdraw, students may process a partial withdrawal (dropping from one or more but not all of their classes) or complete withdrawal (all classes in a term) via the online Course Drop or Withdrawal Request Form,
http://www.uttyler.edu/registrar/registration/withdrawals.php

Student Accessibility and Resources – In accordance with Section 504 of the Rehabilitation Act, Americans with Disabilities Act (ADA) and the ADA Amendments Act (ADAAA) the University offers accommodations to students with learning, physical and/or psychiatric disabilities. If you have a disability, including non-visible disabilities such as chronic diseases, learning disabilities, head injury, PTSD or ADHD, or you have a history of modifications or accommodations in a previous educational environment you are encouraged to contact the Student Accessibility and Resources (SAR) office and schedule an interview with the Accessibility Case Manager/ADA Coordinator, Cynthia Lowery Staples. If you are unsure if the above criteria applies to you, but have questions or concerns please contact the SAR office. For more information or to set up an appointment please visit the SAR office located in the University Center, Room 3150 or call 903.566.7079. You may also send an email to cstaples@uttyler.edu.

APPENDIX A

If circumstances require us to not meet in the classroom, we will instead meet via Zoom at the regularly scheduled times.

Recording of Class Sessions—Class sessions may be recorded by the instructor for use by students enrolled in this course. Recordings that contain personally identifiable information or other information subject to FERPA shall not be shared with individuals not enrolled in this course unless appropriate consent is obtained from all relevant students. Class recordings are reserved only for the use of students enrolled in the course and only for educational purposes. Course recordings should not be shared outside of the course in any form without express permission of the instructor and UT Tyler.

As for the small-team collaborations, there are two parts (presentation and review), as I currently foresee the model, which is subject to change I deem as necessary.

1. The collaboration activities—These are conducted outside of the synchronous course activities. Each team decides whether to collaborate in-person or online.
    a. In the work world, teams within the organizations that are the most advanced in the use of work-at-home models conduct most of their collaborations asynchronously and in writing, using online devices such as Wikis, Google Docs, MS Teams, and Slack.
    b. As of now, I'm not sure the extent to which I will prescribe the platform on which teams in our class will collaborate.
    c. I mention this here because I know that in the world of work, leading organizations prescribe the platform in part for the purpose of consistency and in part because they wish to accumulate collaboration data in a highly structured format that is amenable to text mining, sentiment analysis, affective computing analysis, and so on.
    d. I foresee these data-structuring and analysis techniques becoming commonplace not only in work-at-home contexts but also in study-at-home contexts, where business schools aim to prepare their students for the reality of distributed work, where employers will seek and reward persons who can collaborate via distributed work, and avoid persons who cannot.
2. Presentation and review activities—There will be presenting teams and reviewing teams.
    a. Presenting Team
        i. Each presenting team will create a Word document that provides thoughtful support for its proposed solution, following a model that I will provide.
        ii. The team will video-record its presentation (e.g., via Zoom or Canvas Studio).
        iii. The presentation will feature the use of an artifact (e.g., a PowerPoint document, viewed via screen-share) to support the discussion of the problem and the proposed solution.
        iv. Each team member must participate.
        v. The presenting team will upload to Canvas the video-recorded presentation, the supporting Word document, and the presentation artifact (e.g., PowerPoint document) two instruction days before the scheduled presentation date.
    b. Reviewing Team
        i. For each presentation, there will be a reviewing team.
        ii. The reviewing team will access the presenting team's uploaded materials and prepare questions to ask of the presenting team.
        iii. On the day of the presentation, the reviewing team will interrogate the presenting team's proposed solution via a live, video-captured Zoom session, which I will facilitate actively.
            1. Notice that most of my activities will be in the nature of facilitating these

student interactions, and not lectures. For each course module, I will post instructional materials to Canvas.

iv. Following the colloquy between the presenting team and the reviewing team, the audience of peers will anonymously assess:
    1. the effectiveness of
        a. the presenting team's proposed solution;
        b. the delivery of each presenting student;
    2. the effectiveness of
        a. the reviewing team's interrogation of the proposed solution; and
        b. the questioning of each reviewing student.

3. Anonymized peer assessments—These are formative, i.e., they are intended to inform student reflections, but not for grading purposes. I, as the instructor, will independently assess the performance of the presenting and reviewing teams and their members for grading purposes.

This model is designed to:

1. produce a high degree of student engagement;
2. in the service of using evidence-based, collaborative reasoning;
3. to apply relevant domain knowledge;
4. to communicate a thoughtful proposed solution to a real-world problem;
5. using information and communication technologies;
6. following a study-at-home model that anticipates the work-at-home models that are being adopted across global industry now, in the wake of the COVID-19 disruptions.

APPENDIX B: GUIDANCE FOR COVID-RELATED MATTERS

Information for Classrooms and Laboratories—Students are expected to wear face masks covering their nose and mouth in public settings (including classrooms and laboratories). The UT Tyler community of Patriots views adoption of these practices consistent with its Honor Code (Links to an external site.) and a sign of good citizenship and respectful care of fellow classmates, faculty, and staff.

Students who are feeling ill or experiencing symptoms such as sneezing, coughing, digestive issues (e.g. nausea, diarrhea), or a higher than normal temperature should stay at home and are encouraged to use the UT Tyler COVID-19 Information and Procedures (Links to an external site.)website to review protocols, check symptoms, and report possible exposure. Students needing additional accommodations may contact the Office of Student Accessibility and Resources at University Center 3150, or call (903) 566-7079 or email saroffice@uttyler.edu.

REFERENCES

ArborNetworksEditors. (2017). White Paper: Protect From Encrypted Threats. *Arbor Networks*. Retrieved August 5, 2018, from https://pages.arbornetworks.com/rs/082-KNA-087/images/Protect_from_Encrypted_Threats_WP.pdf

Bauer, H., Scherf, G., & Vondertann, V. (2017). Six ways CEOs can promote cybersecurity in the IoT age. *McKinsey Internet of Things*. Retrieved August 5, 2018, from https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age#0