CSC 444/544/CYEN 406: Applied Cryptography

Course Description: An introduction to the basic theory and practice of cryptographic techniques used in computer security. Topics include encryption, key management, hashing, network security protocols.

Course Outcomes: Upon **successful completion** of this course, students should:

1. Understand the importance of cryptography;
2. Understand what is involved in the implementation of various cryptographic protocols;
3. Implement various hashing and cryptographic functions;
4. Understand the differences between symmetric and asymmetric cryptography;
5. Understand appropriate usage of symmetric and asymmetric cryptography;
6. Understand the math behind various major cryptographic techniques;
7. Write various programs to implement cryptographic principles;
8. Understand the limitations of modern-day cryptography; and
9. Understand common attacks on cryptosystems.

Prerequisite(s): CSC 442 or CYEN 301 (with a **C** or better).

Classroom/Time: IESB 205 / MWF 8:00 – 9:15 AM

Office Hours: Click Here to Schedule an Appointment

Textbook: None. They're way too expensive.

Grades: Your grade for this class will be determined by dividing your total earned points by the total points possible. In general, graded components will fall into the following categories:

Programs:	~30% (50 points each 300 total)
Challenges:	~45% (150 points each 450 total)
Final Project:	~25% (250 points total)

Labs/Challenges: Labs are class periods where students individually follow along on a laptop as the prof is leading a demonstration. Challenges are class periods where teams of students work toward a stated goal. Labs/challenges are typically held on Fridays during normal class time. **You must bring your laptop to all labs/challenges!** Note that there may be other class periods where a laptop will be extremely beneficial.

Graduate Students: Graduate students will be required to complete the challenges individually on a slightly different time frame. Also, each group for group projects will have one graduate student whose responsibility will be to help plan and trouble shoot the group's project. They will act as the team lead in organization.

Students needing testing or classroom accommodations based on a disability are encouraged to discuss those needs with me as soon as possible. For more information, please visit www.latech.edu/ods.

If you are ill, you can get treatment at the Wellness Center in the Lambright Intramural Center building. The nurses there can treat minor illnesses and can give vouchers to see doctors in town for more serious illnesses. Since you have already paid for this service through your fees, there is usually no additional charge. Also, if you sign a HIPPA release form at the time of your visit, they can verify that you were ill and thus you will have an excused absence for missing class.

In accordance with the Academic Honor Code, students pledge the following: "Being a student of higher standards, I pledge to embody the principles of academic integrity." For the Academic Honor Code, please visit http://www.latech.edu/documents/honor-code.pdf.

All Louisiana Tech students are strongly encouraged to enroll and update their contact information in the Emergency Notification System. It takes just a few seconds to ensure you're able to receive important text and voice alerts in the event of a campus emergency. For more information on the Emergency Notification System, please visit http://ert.latech.edu.

COVID-19 Information:

a. Students can access COVID-19-related information, guidelines, FAQs, and policies at Louisiana Tech's website: https://www.latech.edu/coronavirus/.
b. Louisiana Tech's Return to Campus Plan is located at https://www.latech.edu/coronavirus/return-to-campus-plan/. Masks are recommended to be worn indoors on campus. Every member of the Tech Family will need to take personal responsibility for their behavior, which includes wearing masks, maintaining physical distance, washing hands regularly, using proper sneeze and cough practices, helping maintain clean academic and office areas, and monitoring for symptoms of COVID-19.
c. The direct link to the reporting protocol for students is located at https://www.latech.edu/coronavirus/return-to-campus-plan/for-students/. Students can reach out to Stacy Gilbert, Dean of Student Services & Academic Support, at stacyg@latech.edu for help with accommodations and additional information.

d. Failure to comply with the Safety Protocols listed in the Back to Campus Fall 2020 booklet, https://www.latech.edu/documents/2020/07/covid-return-book.pdf/, specifically on pages 5-7 about masks and social distancing, could result in students being in violation of

the Classroom Behavior Policy listed on page 125 of the Student Handbook https://www.latech.edu/documents/2018/09/student-handbook.pdf/.
e. Information and contact numbers and sites for Louisiana Tech Counseling Services are located at: https://www.latech.edu/current-students/student-advancement-affairs/counseling-services/.

In compliance with Acts 635, 637, and 640 of the 2018 Regular Session and Act 382 of the 2019 Regular Session of the Louisiana Legislature and the 2019 Board of Regents Uniform Policy on Hazing, the System reaffirms its policy that any form of hazing of any student enrolled at any institution of the System is prohibited. Violation of this Policy can result in both disciplinary action imposed by the organization and/or institution as well as criminal charges.

In the event that a disaster or other emergency results in campus closure, this course will continue via Moodle. You will be required to login to *moodle.latech.edu* **for further instructions. Please enroll in the** *Emergency Notification System* **to receive official campus updates. You may also refer to** *ert.latech.edu* **for updated information.**

TOPICS COVERED:

- Foundations
- Symmetric cryptography
- Public key cryptography
- One-way functions
- Cryptographic protocols
- Digital signatures
- Miscellaneous protocols
- RSA
- Key management
- Diffie-Hellman key exchange
- SSL/TLS
- Cryptographic random numbers
- Elliptic curve cryptography
- AES
- DES