CS 647 Course Syllabus

Instructor Information

Instructor

Yongming Fan

Email

yongming.fan@bsu.edu

General Information

Description

Introduction of basic principles and applications of cybersecurity. Topics include symmetric and asymmetric encryption and decryption algorithms, hashing techniques, digital certificates, digital signatures, message authentication codes, authentication, malware, and security of systems such as networks, operating systems, software, and databases.

Course Objectives

Upon successfully completing this course, the student should be able to

- Describe symmetric and asymmetric cryptographic algorithms.
- Demonstrate security application development skills.
- Compare key distribution algorithms.
- Compare authentication techniques.
- Explain transport layer security.
- Demonstrate proficiency in the security of systems and applications such as email, networking, database, and operating systems.

Course Topics

- Foundations of cryptography
- Foundations of systems (operating systems and computer networks)
- Hash functions

- Message authentication codes
- Public key infrastructure
- Digital signatures
- Transport layer security
- Access control
- Applications such as firewall, and malware

Prerequisites

CS 601 and CS 602 or permission of the Computer Science Graduate Program Director.

Course Modality and Structure

This course is offered in an online, asynchronous format through Coursera. Course content and assignments are arranged in weekly modules. Each module is composed of the following items: recorded lectures, reading assignments, and scheduled assessments and exams. Students can work through each module's material at their own pace.

Course Alignment Map

Course-level Objective	**Module-level Objective**	**Learning Activities**	**Assessment Measures**
All course objectives	**MO 1.1** Identify how the course is structured **MO 1.3** Navigate the Coursera LMS site and locate key resources. **MO 1.2** Locate key course information, such as the information found on the course syllabus	Read through module pages	
All course objectives	**MO 1.4** Explain security attacks, services, and mechanisms	Read Chapter 1 Watch lecture videos	Assignment 1 Quiz 1 Exam 1

Course-level Objective	Module-level Objective	Learning Activities	Assessment Measures
CO 1 Describe symmetric and asymmetric cryptographic algorithms	**MO 2.1** Execute common mathematical theorems used in cryptography	Read Chapter 2 Watch lecture videos	Assignment 1 Quiz 2 Exam 1 Exam 2
CO 1 Describe symmetric and asymmetric cryptographic algorithms	**MO 3.1** Construct substitution and transposition ciphers to ensure confidentiality	Read Chapter 3 Watch lecture videos	Assignment 2 Assignment 3 Assignment 4 Assignment 6 Quiz 3 Exam 1
CO 1 Describe symmetric and asymmetric cryptographic algorithms	**MO 4.1** Defend design decisions of the Feistel cipher to rationalize the design of future symmetric ciphers	Read Chapter 4 Watch lecture videos	Assignment 2 Assignment 3 Quiz 4 Exam 1
CO 1 Describe symmetric and asymmetric cryptographic algorithms	**MO 4.2** Experiment with multiple DES configurations	Read Chapter 4 Watch lecture videos	Assignment 2 Assignment 3 Quiz 4 Exam 1 Exam 2
CO 1 Describe symmetric and asymmetric	**MO 5.1** Select optimal AES parameters to meet contextual security requirements	Read Chapter 6 Watch lecture videos	Assignment 5 Quiz 5 Exam 2

Course-level Objective	Module-level Objective	Learning Activities	Assessment Measures
cryptographic algorithms			Final Exam
CO 1 Describe symmetric and asymmetric cryptographic algorithms	**MO 6.1** Compare block cipher operation modes	Read Chapter 7 Watch lecture videos	Assignment 5 Quiz 6 Exam 2 Final Exam
CO 1 Describe symmetric and asymmetric cryptographic algorithms	**MO 7.1** Describe asymmetric encryption techniques to achieve confidentialty, integrity, availability, non-repudiation, and authentication	Read Chapter 9 Watch lecture videos	Assignment 5 Assignment 7 Quiz 7 Exam 2
CO 1 Describe symmetric and asymmetric cryptographic algorithms	**MO 7.2** Solve RSA encryption and decryption problems	Read Chapter 9 Watch lecture videos	Assignment 5 Quiz 7 Exam 2 Final Exam
CO 1 Describe symmetric and asymmetric cryptographic algorithms **CO 2** Demonstrate security application development skills	**MO 8.1** Compare and contrast El-Gamal and Diffie-Hellman algorithms	Read Chapter 10, Sections 1-2 Watch lecture videos	Assignment 7 Quiz 8 Exam 2 Final Exam
CO 1 Describe symmetric and asymmetric	**MO 8.2**	Read Chapter 8, Sections 1-5	Quiz 8 Exam 2

Course-level Objective	**Module-level Objective**	**Learning Activities**	**Assessment Measures**
cryptographic algorithms **CO 2** Demonstrate security application development skills	Demonstrate use of random number generators in various cryptographic applications	Watch lecture videos	
CO 2 Demonstrate security application development skills	**MO 9.1** Compare and contrast various hashing algorithms	Read Chapter 11 Watch lecture videos	Assignment 8 Quiz 9 Final Exam
CO 2 Demonstrate security application development skills	**MO 9.2** Construct message authentication codes to ensure sender and data integrity	Read Chapter 12 Sections 1 to 5 Watch lecture videos	Assignment 8 Quiz 10 Final Exam
CO 4 Compare authentication techniques	**MO 10.1** Appraise various approaches to digital signature algorithms to meet contextual security requirements	Read Chapter 13 Sections 1 to 4 Watch lecture videos	Assignment 8 Quiz 10 Final Exam
CO 3 Compare key distirbution algorithms	**MO 11.1** Compare and contrast symmetric and asymmetric key distribution algorithms	Read Chapter 15 Watch lecture videos	Assignment 8 Final Exam
CO 4 Compare authentication techniques	**MO 11.2** Compare user authentication techniques	Read Chapter 16 Section 3 Watch lecture videos	Assignment 8 Final Exam
CO 5 Explain transport layer security	**MO 12.1** Critique design choices of the handshake and session protocol	Read Chapter 17 Watch lecture videos	Quiz 11 Final Exam

Course-level Objective	Module-level Objective	Learning Activities	Assessment Measures
CO 2 Demonstrate security application development skills**CO 6**Demonstrate proficiency in the security of systems and applications such as email, networking, database, and operating systems	**MO 13.1** Differentiate between multiple wireless security protocols	Read Chapter 18 Watch lecture videos	Final Exam
CO 6 Demonstrate proficiency in the security of systems and applications such as email, networking, database, and operating systems	**MO 14.1** Select optimal infrastructure security countermeasures to defend against a variety of cyberattacks	Read Chapter 19 Sections 1 to 3 Watch lecture videos	Final Exam
CO 6 Demonstrate proficiency in the security of systems and applications such as email, networking, database, and operating systems	**MO 14.2** Implement firewall rules to secure networks from malicious traffic	Read Chapter 21 Watch lecture videos	Final Exam
CO 6 Demonstrate proficiency in the security of systems	**MO 15.1** Explain cloud and IoT security mechanisms	Read Chapters 22 and 23	Final Exam

Course-level Objective	Module-level Objective	Learning Activities	Assessment Measures
and applications such as email, networking, database, and operating systems			

Course Time Commitment

At Ball State University, it is expected that students will spend approximately 2 hours of study time for every one credit hour of class. Since this is a 3 credit hour class, you should expect to spend up to 9 hours on this class each module: approximately 3 hours of "in class" work (watching lectures and "live" coding examples, contributing to discussions, completing reflective practice work, and exams when scheduled) plus up to 6 hours per module of study time (reading assignments, writing programming assignments, and related work).

Course Materials

Required Materials

Stallings, William, *Cryptography and Network Security: Principles and Practice, 8th Edition*. New Jersey: Pearson, 2020.

Computer Requirements

All assignments are completed on the Coursera platform in your browser. None of the computing occurs on your device, so if you can access a browser, you should be able to complete the assignments, which must be submitted through the Coursera platform.

Required Prior Knowledge and Technical Skills

You are expected to be familiar with computer programming using the Python language. You are also expected to know data structures and high-school mathematics.

Assessment

Grading Weights

Your grade in the course will be based on the following distribution:

Assessment Tool	**Weight**
Quizzes	15%
Assignments	35%
Exam 1	15%
Exam 2	15%
Final	20%
Total	**100%**

Grading Scale

Most likely the following scale will be used to assign final course grades:

Grade	**Course Average Lower Bound**
A	93%
A-	90%
B+	87%
B	83%
B-	80%
C+	77%
C	73%
C-	70%

Grade	Course Average Lower Bound
D+	67%
D	63%
D-	60%
F	0%

Course Policies and Advice

Communication Policy

Please email all questions to cs.support@bsu.edu. We will respond to all questions within 1-2 business days.

Participation Policy

- This course is designed with weekly activities, discussion, and other activities designed to build a scaffold and improve your understanding over time. In addition to watching the lectures, the best way to learn the course material is to carefully study the assigned readings and complete weekly quizzes, so be sure to keep up with the assignment schedule as much as possible.
- Be sure to log into Coursera frequently. Continuous participation throughout the week is much better for learning than trying to "cram" the whole week's assignments in one sitting. Please try to spread out your work over a few days, to give your brain time to digest what it has learned.

Academic Integrity Policy

All CS 647 work MUST be done individually. Discussion on any topic is encouraged but exchange of answers and code by written or electronic means is strictly prohibited. It is considered dishonest either to read someone else's work or provide a copy of your work to someone else. It is also considered cheating to obtain a copy of our solution before it is posted for everyone to view.

In accordance with BSU policy, anyone discovered cheating will be reported to the Provost's office. Penalties for cheating include but are not limited to a grade of zero on an assignment or exam, a lower letter grade or a failing grade in the class.

We are adamant that cheating in any form will not be tolerated. Even the smallest assignment is better not submitted than if you cheat to complete it.

University Policies

Disability Services Statement

If you need course adaptations or accommodations because of a disability, please contact me as soon as possible. Ball State's Disability Services office coordinates services for students with disabilities; documentation of a disability needs to be on file in that office before any accommodations can be provided. Disability Services can be contacted at 765-285-5293 or **dsd@bsu.edu**.

Diversity Statement

Ball State University aspires to be a university that attracts and retains a diverse faculty, staff and student body. We are committed to ensuring that all members of the community are welcome through valuing the various experiences and worldviews represented at Ball State and among those we serve. We promote a culture of respect and civil discourse as expressed in our Beneficence Pledge. For Bias Incident Response information, please click here or e-mail reportbias@bsu.edu.