CodeHS

Advanced Cybersecurity Syllabus
High School (120-145 contact hours)

Course Overview and Goals

Many agree that cybersecurity is “the next big thing” in K-12 computer science education. As technology expands and the number of connected devices grows, so does the need for security and network experts. With over 300,000 job openings in the field[1], students can expect to learn real-world applications of network and security concepts that will open up a world of opportunities.

The CodeHS Advanced Cybersecurity course is the capstone course of the cybersecurity pathway. In this course, students will learn advanced topics in the field of cybersecurity, including advanced cryptography, networking, risk assessment, and cyber defense.

[1] https://www.nist.gov/system/files/documents/2019/02/07/workforce_demand_111617_final.pdf

Learning Environment: The course utilizes a blended classroom approach. The content is a mix of web-based and physical activities. Students will modify existing code and run it in the browser, investigate cyber-related topics, and reflect on them and discuss them, create digital presentations, and engage in in-person collaborative exercises with classmates. Teachers utilize tools and resources provided by CodeHS to leverage time in the classroom and give focused 1-on-1 attention to students.

Programming Environment: Students modify and run programs in the browser using the CodeHS online editor. Students will be able to modify text-based programs in HTML, JavaScript, SQL, and simulate shell commands. Students will also participate in simulated cyber attacks on safe sites in order to learn how to mitigate cyber attacks. Students will be able to document their processes and discuss best practices for preventing cyber attacks.

Quizzes: Each lesson includes at least one formative short multiple-choice quiz. At the end of each module, students take a summative multiple choice quiz that assesses their knowledge of the concepts covered in the module.

Prerequisites: The Advanced Cybersecurity course is designed as a capstone course in the cybersecurity pathway. Students should have completed The Fundamentals of Cybersecurity course before taking this course.

Technology Requirements: To complete all activities and exercises in this course, students must have access to the 3rd party sites and tools listed here: Advanced Cybersecurity Course Links

More information: Browse the content of this course at https://codehs.com/course/7606

Course Breakdown

Module 1: Advanced Cryptography (4 weeks/20 hours)

Students will apply advanced principles of cryptology. This includes explaining the core concepts of Public Key Infrastructure and hash functions. Students will explore concepts of encrypted email, digital certificates, and private key certificates. They will understand the different types of SSL certificates, the chain of trust and how a Certificate Authority (CA) works.

Browse the full content of this module at https://codehs.com/library/course/7606/module/11554

Objectives / Topics Covered	• Encryption Algorithms • Public Key Encryption • Hash Functions • Asymmetric Encryption • Digital Certificates

Example Assignments / Labs	• Encryption Algorithms
	  ○ What are the key functions of cryptography?
	  ○ What is a block cipher?
	  ○ How many bits are used in each block in the Data Encryption Standard (DES)?
	  ○ How does the Advanced Encryption Standard (AES) compare with the DES?
	  ○ Example activity:
	  ■ What is an advantage of using a key instead of a random substitution?
	  ■ Using the Rail Fence Cipher, encrypt your own message and trade with a partner. See if you can decrypt the message without knowing how many rails your partner used.
	  ■ Is the Pigpen cipher stronger than the Caesar and Mixed Alphabet cipher? Why or why not?
	• Public Key Encryption
	  ○ What are the differences between symmetric and asymmetric encryption?
	  ○ What happens during public key encryption?
	  ○ Example activity:
	  ■ What is REALLY meant by “keys” in the computing world?
	  ■ What kind of number procedure do you need to have to make it impossible for Eve to determine any message sent between Alice and Bob?
	• Hash Functions
	  ○ What is a collision in a hash function?
	  ○ What is password salting?
	  ○ How does modulo math increase the strength of an encryption?
	  ○ Example activity:
	  ■ Why must each “salt” be unique for each password?
	  ■ Develop a simple hash function by changing the math in the function createHash(). Be sure to keep some kind of modulo in your math, so there’s no easy way to calculate information based on the types and quantities of certain characters in any message.
	• Asymmetric Encryption

	○ Man-in-the-middle attacks affect which part of the CIA triad? ○ What is a vulnerability of the Diffie-Hellman's key exchange? ○ Example activity: ■ How is a trapdoor function used in the Diffie-Hellman key exchange? How is this related to RSA encryption? ■ What is OpenPGP? ● Digital Certificates ○ What are the different types of SSL certificates? ○ What is the maximum SSL Certificate duration of validity? ○ What is the chain of trust? ○ How can certificate pinning and stapling help prevent man-in-the-middle attacks? ○ Example activity: ■ Connection: How is using a notary public similar to the use of SSL certificates? ■ Become a Certificate Authority: Create a flyer, commercial, or advertisement promoting your certificate authority service.

Module 2: Project: Steganography (1 week/5 hours)
Students will explore steganography and create their own encryption algorithm to conceal and hide a message within the pixels of an image.

Browse the full content of this module at https://codehs.com/library/course/7606/module/13233

Objectives / Topics Covered	● Steganography ● Data Hiding and Extraction ● Encryption Algorithms
Example Assignments / Labs	● Hide a message! Students will create their own pixel picture using a web-based tool to hide a message in using the tool. They will change the hexadecimal values just slightly according to an encryption algorithm that they have created to hide their message!

Module 3: Advanced Networking (4 weeks/20 hours)
Students will explore and research network infrastructures and network security. They will demonstrate how to set up a virtual private network (VPN), and design and configure different types of networks. Students will also explain firewalls and how to initiate port scans.

Browse the full content of this module at https://codehs.com/library/course/7606/module/11562

Objectives / Topics Covered	● Advanced Devices ● Environmental Controls ● Protocols and Standards ● Private Networks ● Mobile Devices ● Access Control
Example Assignments / Labs	● Advanced Devices ○ What is a load balancer? ○ Which actions could be marked as suspicious when using an intrusion detection system (IDS)?

	○ What are the differences between an IDS and an IPS? ○ What devices can be used to block unwanted Internet traffic? ○ Example Activity: ■ What are the main functions of network administrators and how do they support each part of the CIA Triad? ■ Sketch and label a network diagram that fulfills the listed requirements. Include a short explanation of each device used in the network along with its main purpose. ● Environmental Controls ○ What environmental controls are used in computer systems? ○ What is the potential danger of an environment in which the humidity is too low or too high? ○ What security measures are designed to assist with electrical issues? ○ Example activity: ■ What are the physical security measures that are implemented at your school? What do you think could be added? ■ You are tasked with designing the security system for a top-secret government building. Be sure to use a range of different security measures. ● Protocols and Standards ○ What are the protocols used in sending and receiving emails? ○ What is the difference between TCP and UDP? ○ What are the different wireless standards? ○ Example activity: ■ What frequency band(s) can be used with the 801.11ax standard? ■ What is a MU-MIMO device and how does it help the range of the signal? ● Private Networks ○ What is a NAT device used for? ○ How does MAC filtering work? ○ How is a DMZ utilized? ○ What protocols are used in the implementation of a VPN? ○ Example Activity ■ What are the benefits and potential negative consequences of VPNs? ■ Sketch a sitemap for a company intranet along with the permissions needed for each page. ■ Draw a diagram that represents the network setup that will be implemented for the local coffee shop. Be sure to include a variety of security measures such as firewalls, a NAT device, MAC filtering, a DMZ, etc. ● Mobile Devices ○ What security measures can be used on a mobile device? ○ Why is it important to set up a mobile device management policy for a company? ○ Example activity: ■ What are some concerns that might arise from storing facial recognition data on the Apple A11 bionic chip? ■ Do the benefits of BYOD policies outweigh the challenges? Provide evidence to support your answer.

	● Access Control ○ What is RADIUS? ○ What is the importance in securing authentication, authorization, and accounting management? ○ Example activity: ■ What are some advantages of using the RADIUS protocol on a network? How can it support overall network security? ■ Why is the AAA protocol important in network security?

Module 4: Project: IT Professional (2-3 weeks/10-15 hours)
In this project, students will explore cybersecurity career pathways and build skills that will be needed within these fields such as communication.

Browse the full content of this module at https://codehs.com/library/course/7606/module/13129

Objectives / Topics Covered	● Cybersecurity Career Pathways ● Customer Service and Communication ● Contributing to a Knowledge Base ● Creating an Instructional Video
Example Assignments / Labs	● Act it out! Pair up with a partner and create a short script of a customer support scenario based on a common mobile device issue. ● Write a KB Article: Create an internal knowledge base article that will be shared with other technicians. ● Star in a Video! Create a 2-5 minute video tutorial based on a common mobile device issue

Module 5: Cyber Defense (4 weeks/20 hours)
Students will explore different types of network attacks and how to build up security walls to defend against them.

Browse the full content of this module at https://codehs.com/library/course/7606/module/11563

Objectives / Topics Covered	● Network Attacks ● Malware Types and Prevention ● Common Network Attacks ● Additional Attacks ● Cross-Site Scripting ● Internal Threats
Example Assignments / Labs	● Network Attacks ○ What is the difference between a threat, a vulnerability and an exploit? ○ What do cyberattacks commonly take advantage of? ○ Example activity: ■ What are the open ports designated for? ■ What do you notice about the commonly attacked ports and the open ports? ● Malware Types and Prevention ○ What is the difference between anti-malware and antivirus software? ○ What is a virus, work, trojan, rootkit? ○ Example activity:

	■ What type of built-in malware protection does your operating system provide? ■ View all of the running processes on your computer. ● Common Network Attacks ○ What is DoS and DDoS? ○ What is spoofing and why can it be dangerous? ○ Example activity: ■ What makes social engineering such an effective technique for hackers? ■ Does the IoT make us more or less vulnerable to DDoS attacks? ● Additional Attacks ○ What is a rainbow table? ○ What is a zero-day attack? ○ What is a botnet and how are they used? ○ Example activity: ■ Explore the United States Computer Emergency Readiness Team (US-CERT) web page and draw conclusions about the current environment of cyber threats. ● Cross-Site Scripting ○ How does XSS attack a website? ○ Who is the victim in an XSS attack? ○ Example activity: ■ Try some basic XSS on the Google's Tutorial for XSS site. ■ What are some ways to detect XSS vulnerabilities on websites? ● Internal Threats ○ What is the main function of UEFI? ○ What can you do to prevent someone from booting an alternative operating system? ○ What is data loss prevention? ○ Example activity: ■ Explore your computer's BIOS/UEFI! ■ Which data breaches can be prevented by DLP tools?

Module 6: Project: Security Assessment Report (1 week/5 hours)
Students complete a project that has them test a website for vulnerabilities and write a security assessment report based on their findings.

Browse the full content of this module at https://codehs.com/library/course/7606/module/13078

Objectives / Topics Covered	● Project: Security Assessment Report
Example Assignments / Labs	● Project: Security Assessment Report ○ XSS Testing ○ Create a Security Assessment Report ○ Project Reflection

Module 7: Project: Put it in Writing! (2-3 weeks/10-15 hours)
In this project, students will develop a training policy that informs employees on matters of network security and details the company policy on preventative measures employees should take.

Browse the full content of this module at https://codehs.com/library/course/7606/module/13131

Objectives / Topics Covered	• User Training • Incident Response Plans • Data Policy and Privacy • Change Management
Example Assignments / Labs	• Develop a training policy that informs employees on matters of network security. • Create an Incidence Response Plan. • Develop a strong data policy for a company. • Develop a change management plan to ensure that the new policy is adopted and implemented by the team effectively.

Module 8: Risk Management (4 weeks/20 hours)
Students will demonstrate skills in conducting vulnerability scans and recognizing vulnerabilities in security systems. They will conduct a security audit and examine port scanning, packet sniffing, and proxy servers to discover exploits in a system. Students will recommend security measures to mitigate the vulnerabilities.

Browse the full content of this module at https://codehs.com/library/course/7606/module/11564

Objectives / Topics Covered	• Identifying Risks • Assessing Risks • Risk Response • Penetration Testing

Example Assignments / Labs	• Identifying Risks
	  ○ What are the steps of a risk assessment?
	  ○ What potential risks can be checked by a vulnerability scan?
	  ○ How is packet sniffing and password cracking used in a legal manner?
	  ○ Example Activity:
	  ■ What information can be determined by an IP address?
	  ■ Create a “story” using the data shown of what was happening during this packet transfer.
	  ■ Why is past data important in trying to access how to best set up a cyber defense system for the present?
	• Assessing Risks
	  ○ What is a race condition?
	  ○ What is error handling and input handling? Why is input validation important?
	  ○ What is buffer overflow and integer overflow?
	  ○ Example Activity:
	  ■ Draft an argument that insists upon the importance of upgrading a system that has reached its end-of-life.
	  ■ Read a scenario and access the level of risk.
	  ■ Examine (and fix) poor input and error handling.
	• Risk Response
	  ○ What are some risk response strategies?

	○ How do you calculate the SLE and ALE of a threat event? ○ How do you effectively and efficiently mitigate risk? ○ Example activity: ■ Read a sample assessment report. What types of methods did the assessors use to collect data? Do you feel this report provides you with sufficient information to determine priorities and next steps? ■ What role might chaos engineering play in risk assessment and response? ● Penetration Testing ○ What are the stages of penetration testing? ○ What tools are used in passive reconnaissance? ○ What is an escalation of privilege? ○ Example activity: ■

Module 9: Project: The Game of Risk (2-3 weeks/10-15 hours)
In this project, students will design and create a board game or a card game that will help players to identify randomized security vulnerabilities and their appropriate defenses.

Browse the full content of this module at https://codehs.com/library/course/7606/module/13132

Objectives / Topics Covered	● Quantitative and Qualitative SLE ● Prototypes ● Testing
Example Assignments / Labs	● Create a Game: Students will design and create a board game that will help players to identify randomized security vulnerabilities and their appropriate defenses. They will create a prototype and test the game to receive feedback to consider before building their final game.

Supplementary Unit Guide:
These units can be used during the course for added practice or after the course has been completed for further review.

Supplementary Unit	**Prerequisite/Recommended Unit(s)**	**# of activities**
Cryptocurrency - Blockchain - Hashing - Proof of Work - Cryptocurrencies - Bltcoin	No prerequisites	62
SQL Part II: The SQL - Filtering - Ordering - Renaming - Joining	Software Security	35
Web Development - HTML	No prerequisites	75

- Formatting Text - Links, Images, Lists, Tables - CSS by Tag, Class, ID		
Midterm	Modules Covered: ● Advanced Cryptography ● Advanced Networking	1
Final	Modules Covered: ● Advanced Cryptography ● Advanced Networking ● Cyber Defense ● Risk Management	1