Advanced Cybersecurity Syllabus

High School (145 Contact Hours)

Course Overview and Goals

In this Advanced Cryptography course, students build on their foundational cybersecurity knowledge to explore complex concepts in data protection, secure communications, and threat defense. Through interactive lessons, hands-on coding, and investigative projects, students uncover how data is protected, communications verified, and cyber threats mitigated. They'll take on the roles of cryptographers, forensic analysts, and network architects as they tackle real-world security challenges and engineer creative solutions. With projects like building steganographic tools and crafting security policies, students gain both technical expertise and critical thinking skills for the digital age.

Learning Environment

The course utilizes a blended classroom approach. The content is a mix of web-based and physical activities. Each module of the course is broken down into lessons. Lessons are composed of short video tutorials, interactive learning pages, quizzes, explorations, simulations, and free-response prompts. Each module ends with a comprehensive quiz that assesses students' mastery of that module's material.

Programming Environment

In the programming and database modules, students modify and run programs in the browser using the CodeHS online editor. Students will be able to modify text-based programs in Python and SQL and simulate shell commands.

Prerequisites

The Advanced Cybersecurity course is an advanced course for high school students. Students should take this course after successfully completing the Fundamentals of Cybersecurity (or equivalent) 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/26081/overview

Course Breakdown

Module 1: Advanced Cryptography (2 weeks/10 hours)

In this module, students will deepen their understanding of modern cryptographic systems by exploring advanced concepts like public key encryption, hashing, digital certificates, and password salting. Through lessons, articles, code exercises, and creative assignments, they'll learn how encryption secures data, how

hashing algorithms are constructed and attacked, and how secure communications are verified and maintained online.

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

Example Assignments	• 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 ciphers? 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?
	• 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?
	• 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:
	  ■ Become a Certificate Authority: Create a flyer, commercial, or advertisement promoting your certificate authority service.

Module 2: Project: Steganography (1 week/5 hours)

In this module, students will explore how steganography allows messages to be hidden in plain sight, often within images, text, or other media. Students will learn real-world applications of this practice, analyze encryption methods, and create their own image-based steganography projects. The module culminates in peer-to-peer decoding and reflection activities.

Objectives / Topics Covered	• Steganography • Data Hiding and Extraction • Encryption Algorithms • Peer Collaboration
Example Assignments	• 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: Cyber Defense (3 weeks/15 hours)

In this module, students will investigate the various forms of cyberattacks and the methods used to carry them out. They will distinguish between threats, vulnerabilities, and exploits, analyze different types of malware and network attacks, and explore real-world prevention strategies.

Objectives / Topics Covered	• Network Attacks • Malware Types and Prevention • Common Network Attacks • Additional Attacks • Cross-Site Scripting • Internal Threats

Example Assignments	• 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 are a virus, worm, trojan, and 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 4: Threats and Security Principles (2 weeks/10 hours)

In this module, students will explore foundational security concepts and apply them through real-world scenarios and simulations. They will learn to distinguish between threats, vulnerabilities, and exploits; investigate actual data breaches; evaluate ethical concerns; and examine how protocols and baseline security measures defend against attacks.

Objectives / Topics Covered	• Threats, Vulnerabilities & Exploits • Cyber Case Investigation • Security Breaches & Ethics • Security Baselines & Policies • Network Defenses & Protocols

Example Assignments	• Cyber Case Investigation
	  ◦ Students role-play as Red Team (attacker) and Blue Team (defender) to:
	  ▪ Research a real cyberattack
	  ▪ Analyze threats and vulnerabilities
	  ▪ Suggest prevention strategies
	• Research: Unethical Security Breaches
	  ◦ Analyze a breach and its impacts.
	• Research: High Profile Breach
	  ◦ Identify threats, vulnerabilities, and mitigations.
	• Security Skit / Roleplay
	  ◦ Scenarios covering password policies, guest account misuse, and administrator account settings
	• Lab: Anti-virus Software Installation

	○ Students will research, install, configure, and document the process of setting up anti-virus software to secure a system.

Module 5: Project: Digital Forensics (1 week/5 hours)

In this project, students will step into the role of digital forensic investigators, using real-world techniques to analyze system logs, metadata, and image data. Through hands-on scenarios, they will learn how digital footprints can be uncovered and interpreted to solve cyber incidents, identify misuse, and verify or disprove claims in both criminal and non-criminal investigations.

Objectives / Topics Covered	● Network Log Analysis ● File Metadata Inspection ● Image Forensics via EXIF Data
Example Assignments	● Investigate SSH Intrusion ○ Which login attempts were successful ○ What usernames and techniques were used ○ Recommendations to prevent future attacks ● Analyze Word Document Metadata ○ Use simulated file properties to investigate Jacob's claim of authorship. Determine: ■ Original creation date ■ Author and last modifier ■ Editing duration ● Examine a photo's EXIF data to verify the following: ○ Was the image taken with a specific iPhone? ○ Was flash used? ○ Was the image taken indoors? ○ Where (geographically) was the photo taken? ● Write a Forensics Report ○ For any of the three cases, write a formal forensic report that includes: ■ Evidence summary ■ Timeline of key events ■ Your verdict (support/refute the claim) ■ Suggested technical and policy improvements

Module 6: Advanced Networking (2 weeks/10 hours)

In this module, 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.

Objectives / Topics Covered	● Advanced Devices ● Environmental Controls ● Protocols and Standards ● Private Networks ● Mobile Devices ● Access Control
Example Assignments	● 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. ● 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 7: Networking Infrastructure (3 weeks/15 hours)

In this module, students explore the foundational elements that make up digital communication systems, guiding students through the history, components, and security of computer networks. Students analyze network models, services, and tools, and simulate both theoretical and practical aspects of network design and security.

Objectives / Topics Covered	• Internet Evolution & Network Growth • Network Models & Architectures • Networking Services & Protocols • Network Security & Design

Example Assignments	• OS Security Showdown Cards
	  ○ Students create digital "battle stat" cards for 4 major operating systems (Windows, macOS, Linux, Unix). Each card includes:
	  ■ OS nickname, logo, usage stats
	  ■ Security strengths and weaknesses
	  ■ Ratings on authentication, encryption, malware resistance
	  ■ Real-world use case (e.g., hospitals, schools)
	• Packet Simulation & Analysis
	  ○ Students run a simulated packet analyzer tool that mimics traffic between clients and servers. They adjust:
	  ■ Duration and packet flow rate
	  ■ Anomaly injection (e.g., suspicious packets)
	  ■ Filter for specific protocols or IPs
	• Secure Cyberville Blueprint
	  ○ Design and defend a full network infrastructure for a fictional town:
	  ■ Diagram includes DNS, DHCP, AD, file servers
	  ■ Visual layout with IP ranges and domain names
	  ■ Written justification of decisions and security protections
	  ■ Reflection on risks and failure points
	• Lab: Windows Networking
	  ○ Students will explore Windows networking settings and how they can configure and customize their online experience.
	• Lab: Network Protocols
	  ○ Students are introduced to CSMA/CD and CSMA/CA, two network protocols designed to manage data transmission and prevent or handle collisions on shared communication channels.
	• Lab: Setting up Remote Access
	  ○ Students will create a beginner-friendly tutorial on how to turn a Windows Server into a router and set up Routing Information Protocol (RIP) for network communication.

Module 8: Project: The Inside Scoop on LANs (2 weeks/10 hours)

In this project, students will create a "magazine" that explains key concepts about Local Area Networks (LANs), topologies, Ethernet standards, and LAN cabling. Students will research and present the information in a magazine-style layout with sections, images, and creative design.

Topics Covered	• LAN Methodologies • Network Topologies • Perimeter Networks (DMZ) • Ethernet Standards

	• LAN Cabling

Example Assignments	• Advice Column
	  ○ Students are given three “reader questions.” They will create a response for each question and provide advice on the best network methodology for the scenario.
	• Product Review
	  ○ Students will create a "product review" for a few LAN topologies that includes details about what the product does well, any problems it might have, and whether it meets expectations

Module 9: Risk Management (2 weeks/10 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.

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

Example Assignments	• 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 assess 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 assess 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?

Module 10: Project: Put it in Writing! (2 weeks/10 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.

Objectives / Topics Covered	● User Training ● Incident Response Plans ● Data Policy and Privacy ● Change Management
Example Assignments	● Develop a training policy that informs employees on matters of network security. ● Create an Incident 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 11: Databases (2 weeks/10 hours)

In this module, students will explore the fundamentals of SQL and relational databases, including structuring data into tables and writing basic SELECT queries with filters. They will then deepen their skills by practicing advanced filtering, sorting, and data presentation using logical operators, compound conditions, and clauses like ORDER BY and AS. Finally, students will learn how to join multiple tables to solve complex data problems and simulate real-world database scenarios.

Topics Covered	● Structuring Data in SQL ● Basic Querying in SQL using SELECT ● Filtering Queries in SQL using WHERE ● Advanced Filters (BETWEEN, LIKE, IN) ● Ordering Results using ORDER BY ● Renaming Fields using AS ● Joining Tables using JOIN
Example Assignments	● Harry Potter Names ○ Return a table with the first_name and last_name of everyone in the Person table. ● The Patil in Ravenclaw ○ Write a query that returns the first name of a student whose last name is "Patil" and is in the Ravenclaw house. ● Using BETWEEN ○ Find the first and last names of all people whose ID is between 35 and 45. ● Compound Queries with BETWEEN ○ Find the first and last names of all people with IDs between 67 and

	77 who are in Slytherin. ● Sort the P Names ○ Return a list of all the first and last names of people whose last name starts with P. ○ Order the list by last name alphabetically and then by first name in reverse alphabetical order. ● Courses and Professors ○ Return a list of all courses along with the first and last names of the professors who teach them. ○ Sort the results alphabetically by course name. ● Defense Students by House ○ Return a class roster with last name, first name, and house for the Defense Against the Dark Arts course. ○ Sort the results first by house, then by last name, then by first name (all alphabetically).

Module 12: Programming in Python (2 weeks/10 hours)

In this module, students are introduced to the fundamentals of programming by learning how to write basic code in Python using print statements, variables, user input, and arithmetic expressions. They'll explore data types, string operations, comments, and the role of programming languages in creating interactive programs.

Objectives / Topics Covered	● Printing ● Variables ● Types ● User Input ● Converting Input Types ● Arithmetic Expressions ● String Operators ● Comments ● Programming Languages
Example Assignments	● Printing ○ Print messages to the console ● Variables ○ Create variables of different types, and print them to the console. ● Types ○ Investigate the types of different variables ○ Convert between types ● Arithmetic Expressions & Converting Input Types ○ Age in One Year - Ask the user how old they are, and tell them how old they will be in one year ○ Rectangle, part 1 - Make variables for length and width and compute area and perimeter ○ Rectangle, part 2 - Ask the user for length and width, and compute area and perimeter

Module 13: Decisions in Programming (2 weeks/10 hours)

In this module, students expand their programming skills by working with Boolean values, logical and comparison operators, and if statements to create decision-making programs. They apply their understanding to secure coding practices and explore how programming decisions align with real-world cybersecurity policies and principles.

Objectives / Topics Covered	● If Statements ● Boolean Values ● Logical Operators ● Comparison Operators ● Floating Point Numbers
Example Assignments	● If statements and boolean values ○ Is it raining? - Write a program that uses a boolean variable to determine whether or not it is raining ● Boolean operators and expressions ○ Boolean variable - Take a variable and use it in an if statement ○ Legally allowed to vote - User reports age and the program tells them whether or not they can vote in the US ○ Transaction - The user reports the balance and deposit/withdrawal, and the program prints a new balance or error ○ Recipe - Ask the user for ingredients, amounts per serving, and number of servings, and report the total amount of each ingredient needed

Module 14: Project: The Engineering Design Process (3 weeks/15 hours)

In this project, students will learn the theory and practice of the engineering design process. This project allows students to think creatively about the applications of the concepts covered in the course and create something of personal value.

Topics Covered	● Design Thinking ● Prototyping ● Testing ● Project Prep and Development
Example Assignments	● Using Data ○ Creating a Survey ○ Data Cleaning ○ Comparing Datasets ○ Drawing Conclusions ● Prototyping and User Testing ○ Wizard of Oz Prototyping ○ How to User Test Responses