Unit 3 - Cryptography

Content Area: **Computer Science**
Course(s):
Time Period: **Marking Period 1**
Length: **4-5 weeks**
Status: **Published**

Brief Summary of Unit

This unit starts with looking at the rationale for cryptography, framing the discussion in a historical context beginning with Caesar ciphers, and progressing through modern-day methods. The need for cryptography is tied to the CIA triad, and students see how some ciphers are easily "cracked" through mathematical analysis. Students then learn about the difference between symmetric and asymmetric encryption, and the necessity of asymmetric encryption for safe-guarding information transmitted through the internet. The unit concludes with an introduction to hash functions, and the opportunity for students to construct some simple hash functions.

Revised November 2023

Standards

- TECH.8.1.12.B.CS1
- TECH.8.1.12.D.2
- TECH.8.1.12.D.5
- TECH.8.1.12.D.CS1
- TECH.8.1.12.E.CS4
- TECH.8.1.12.F.CS3
- TECH.8.2.12.A.CS1
- TECH.8.2.12.B.CS1
- TECH.8.2.12.B.CS4
- TECH.8.2.12.E.1
- TECH.8.2.12.E.4

CS.9-12.AP	Algorithms & Programming
CS.9-12.CS	Computing Systems
CS.9-12.ED	Engineering Design
CS.9-12.IC	Impacts of Computing
CS.9-12.NT	Nature of Technology
CS.9-12.ETW	Effects of Technology on the Natural World
	Individuals select digital tools and design automated processes to collect, transform,

generalize, simplify, and present large data sets in different ways to influence how other people interpret and understand the underlying information.

Transfer

- Topics in this unit require students to examine an encryption method, a method that will scramble data, and evaluate its efficacy. Students learn to evaluate the usefulness of these methods based on how easy they are to crack. This process helps students to learn that critical thinking and analysis can help them make decisions about the best decisions to make given a particular scenario. This skill is useful in many aspects of life. Additionally, through studying public key encryption, students gain a better idea of how they are protected when they visit certain Internet sites. Knowledge of this topic will help students stay safe when they browse the Internet on various networks. Depending on the students' backgrounds, it may be advisable to introduce binary, and how it relates to the topics at hand.

Essential Questions

- How does binary and the computer's use of bits relate to the successful implementation and scalability of cryptographic methods?
- How does cryptography help to maintain the CIA triad?
- What are some ways to crack a substitution cipher? Under what circumstances are these cracking methods effective?
- What is cryptography? Cryptology? Cryptanalysis?
- What was a major historical force that was responsible for advancing cryptography?
- Why is symmetric encryption insufficient for encrypting Internet data? How does asymmetric encryption remedy the problems posed by symmetric encryption?

Essential Understandings

- Asymmetric encryption is better for Internet encryption because the sender and recipient do not have to communicate about a shared key. Communicating about a shared key would require the electronic analogy to an in-person meeting, which is infeasible for computers on a network.
- Cryptography is the study and practice of encrypting transmitted information so that only authorized people may view it
- Cryptography maintains the CIA triad by helping to maintain the Confidentiality and Integrity of data sent on a network
- Historically, military communication was a driving force behind developing cryptographic techniques
- Ideal hash functions are non-invertible, except by brute force. The nature of the function makes brute force cracking infeasible. Ideal hash functions also have no collisions (no two inputs have the same hash value). This helps to detect if a transmitted message has been altered.
- Mathematically, increasing the length of an encryption key by even one digit will double the number of possibilities a hacker would have to try in a brute force attempt to find the key. In practice, electronic encryption keys are very lengthy, so this doubling effect helps to make encryption methods much more secure.
- Substitution ciphers can be cracked by brute force or frequency analysis. These methods work well for smaller key possibilities, and in the case of frequency analysis, when the same key is used for all letters in a text message.

Students Will Know

- Computers work in binary, perceiving everything in 1s and 0s
- How substitution ciphers can be cracked
- How substitution ciphers work
- How to carry out modulo division
- The basis of asymmetric encryption, and as a specific instance, the basis of public key encryption
- The basis of symmetric encryption
- The ideal characteristics of a hash function

Students Will Be Skilled At

- Converting between decimal and binary
- Cracking certain kinds of substitution ciphers
- Encrypting/decrypting messages with substitution ciphers
- Explaining/using asymmetric encryption, specifically public key encryption, to transmit a message securely
- Explaining/using symmetric encryption to transmit a message securely
- Using knowledge of ideal hash functions to identify if a given hash function is ideal
- Using modulo division to construct a simple hash function

Evidence/Performance Tasks

Assessments

- Formative: Daily assessments using examples from class notes and CodeHS.com, AP Classroom/Albert Checks for Understanding
- Summative: Teacher-created assessments/projects and CodeHS Computer Science Projects, AP Classroom/Albert Unit Assessments
- Benchmark: Check for understanding benchmark assessments on CodeHS, AP Classroom/Albert/Khan Academy Diagnostics
- Alternative Assessments: Student-centered activities such as a doorbell coding project, game design projects, and other activities involving real world applications

- Answer essential questions
- Class discussion of daily topic
- Classwork and homework that assess the essential questions

- Provide alternative means of assessments for certain students
- Teacher Observation
- Tests and quizzes that assess the essential questions
- Written assignments that assess the essential questions that involves providing explanations

Learning Plan

- Advanced Cryptography (Symmetric vs. Asymmetric & Public Key Encryption)
- Basic Cryptography Systems
- Building a Simple Hash Function Using Modulo Division
- Cracking Basic Cryptography Systems
- Cryptography, Cryptology, Cryptanalysis
- Current event presentations about cryptography
- Examining Hash Functions
- History of Cryptography
- Introduction to Binary and Bits
- Modulo Division
- Relation Between Cryptography and the CIA Triad
- Viginere Cypher

Materials

Core instructional materials: Core Book List

Supplemental materials: CodeHS

- Computers
- Teacher created activiites
- Teacher created notes
- Website such as codehs.com for content
- Websites to research current events

Suggested Strategies for Modifications

Possible accommodations/modification for Introduction to Cybersecurity