Shift Ciphers and Machine Learning

Unit Name: **Shifted Ciphers and Machine Learning**	**Content Area:** Computer Science	**Duration: 2 - 4 weeks**

Essential Question(s):

1. Why is encryption important for everyday life on the internet?
2. How do we write a program that can encode/decode using shift ciphers?
3. How does training our program simulate machine learning ?

Assessments

Pre-Assessment:	**Summative Assessments:**
Pre-unit survey that determines perceived comfort level with algorithms, encryption, and machine learning concepts.	• Program to encode/decode shift ciphers • One-pager about machine learning research • Post-unit survey

CSTA Standards

Identifier	**Standard**
3B-AP-10	Use and adapt classic algorithms to solve computational problems.
3B-AP-11	Evaluate algorithms in terms of their efficiency, correctness, and clarity.
3B-AP-12	Compare and contrast fundamental data structures and their uses.
3B-AP-13	Illustrate the flow of execution of a recursive algorithm.
3B-AP-14	Construct solutions to problems using student-created components, such as procedures, modules and/or objects.
3B-AP-18	Explain security issues that might lead to compromised computer programs.
3B-AP-21	Develop and use a series of test cases to verify that a program performs according to its design specifications.
3B-AP-22	Modify an existing program to add additional functionality and discuss intended and unintended implications
3B-IC-25	Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society.
3B-IC-26	Evaluate the impact of equity, access, and influence on the distribution of computing resources in a global society.
3B-IC-27	Predict how computational innovations that have revolutionized aspects of our culture might evolve.
3B-NI-04	Compare ways software developers protect devices and information from unauthorized access.

Learning Plan

Focus Questions	**Academic Tasks**	**DOK (1-4)**	**Notes**	**Resources**	**Academic and Discipline-Specific Vocabulary**	**Differentiation ideas**
Why is encryption important for everyday life on the internet? How do you encode secret messages? (1-2 periods)	Students are given an encoded message to decipher.	**2**	At the beginning of the lesson, students are asked to respond to a prompt about what things they or other people keep secret and why. This leads to a discussion about why we might encrypt the information we place online. During the unplugged lesson, students are introduced to a message encoded using a shift	Code.org Lesson Reading and questions Create your own shift cipher wheel	Caesar Cipher, Cipher, Cracking encryption, Decryption, Encryption, Random Substitution Cipher	Keep track of new vocabulary on a word wall or in a notebook. Demonstrate how to create a cipher using the wheel provided. Extension activity for students to experiment with substitution ciphers.
	Students read an excerpt about encryption.	**1**				
	Pairs answer questions about the reading.	**3**				
	Students write encoded messages for other students to break.	**4**				

			(Caesar) cipher. Later, they'll learn about the history of ciphers and how to decrypt shift ciphers. Finally, they'll make their own encoded messages for another student to decrypt by creating their own shift cipher.			
How do you break simple encryptions? What are the weaknesses and security flaws on shift ciphers? (1-2 periods)	Discovery-based introduction to the online widget	**3**	In this lesson, students move to an online setting to experiment with online widgets that assist in the visualization of shift and substitution cipher. Students will understand that substitution and shift ciphers can be difficult to decrypt by hand, but with computers are very easy to crack, prepping them to create their own program to decode shift ciphers.	Code.org Lesson	Caesar Cipher, Cipher, Cracking encryption, Decryption, Encryption, Random Substitution Cipher, Random Substitution Cipher	Allow time for students to experiment with the widget. Have a student or pair explain briefly how the widget works.
	Students work in pairs to crack a Caesar Cipher using the online widget	**3**				
	Students answer review questions about simple encryption	**2**				
How do we develop a plan before beginning our coding? What does our program need to do? What methods are needed in our program? What data structures are needed for our program to run? (2-4 periods)	Students outline what the program needs to do.	**1**	The timing of this section will vary depending on the experience level students have with algorithms, data structures, and subgoal labeling. See the "differentiation" section to the right for scaffolds and modifications.	Planning a programming project (article) Planning with pseudo-code (video) Top down design (article)	Shift cipher Caesar cipher Pseudo code Encrypt Decrypt Methods Data structures Subgoal labeling	1. Offer students a partially completed program outline and have students work to complete the remaining parts of the outline. 2. Have students generate 3 methods that they think will be useful in this program, then have students collaborate in groups/full class to merge all methods. 3. List all discussed data structures and methods and have students try to match methods with data structures that can help. 4. Students choose 2-3 methods to write subgoal labels.
	Students create a list of methods needed for the program to run successfully.	**2**				
	Students determine the data structures required for coding.	**3**				
	Students subgoal label each method for future use.	**4**				

How can students work as a team to code their program? How can students test their program? (5-10 periods)	Students work to complete their program methods.	**4**	The implementation and execution of this program may look very different depending on the group of students working on the project. Students can write programs that solve shift ciphers, with or without training, depending on their skill level and time given for the project. Some students may allow for generated frequency tables using input, while others may hard code the frequencies based on real frequencies looked up online. Students who do not implement machine learning should at least consider how it might happen, even if they do not write code to implement it.	Top 10 Tips for Efficient Team Coding (article)	Shift cipher Caesar cipher Pseudo code Encrypt Decrypt Methods Data structures Subgoal labeling	Offer students test cases to try with their program to identify bugs Code review days Allow for assumptions to be made so code works for specific cases and not **all** cases (ex: assume no symbols, assume lowercase, etc.) Allow training component to be written in pseudocode or code
	Students test each method during and after writing to verify usability.	**3**				
	Students review code written by other group members to discuss algorithms and logic.	**3**				
	Students work to run multiple methods together in the main method with test input to decrypt a message.	**2**				
What is Machine Learning? (1-2 period)	YouTube video: Machine Learning Basics. (8 m) https://www.youtube.com/watch?v=ukzFI9rgwfU Has a quick quiz (w/o answers) towards the end and a request for everyday examples.	**1**	We can use the end of the unit to look back and use it as a jumping point to introduce M/L. Even though our code is not quite M/L, the idea of "training" the program with text can be used to introduce M/L. Three types: • Supervised Learning - Labeled data • Unsupervised Learning - Unlabeled data • Reinforcement Learning -	Wikipedia: https://en.wikipedia.org/wiki/Machine_learning Slide show: http://www.cs.cmu.edu/afs/cs.cmu.edu/project/theo-20/www/mlbook/ch1.pdf (specifically the second slide is simple and appropriate)	An **algorithm** is a well-defined procedure that allows a computer to solve a problem **Machine learning (M/L)** is the study of computer algorithms that improve through experience. It is a subset of artificial intelligence. Machine learning algorithms build a model based on data known as "training data".	Even though students at this point know what an algorithm is, repeating the definition will help Els and any student new to CS. A graphic organizer with specific questions to answer when researching the material. E.g. What is M/L? Who started the concept of M/L? When was M/L first introduced? What specific evolution of M/L can you name? What common products used today use M/L? Slides have a lower cognitive load than academic text. Provide resources to the students. Challenge: Why do I say our code is not quite M/L?
	Review concepts and definitions.	**2**				
	Ask for examples and have some handy to show.	**3**				
	Mini-research in small groups. Students produce one-pager reports on the history of M/L and how it is used today.	**4**				

What are the considerations we need to have with M/L? (1 period)	TEDX talk: How I'm fighting bias in algorithms (8 min) https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms	**1**	Our code exemplifies the most important concepts about training data and bias which are critical for students. Issues and examples for our code: ● Too little data (a few words) ● Incorrect data (a different language) ● Diversity (the same letter many times)	TED & TEDX have many AI talks which can be used to address M/L, e.g. Can Robots be creative? (5 m) https://www.ted.com/talks/gil_weinberg_can_robots_be_creative You can also search Youtube for interviews addressing AI issues, e.g. Machine Learning Basics https://www.youtube.com/watch?v=ukzFI9rgwfU	(same plus) Bias - prejudice **in favor of or against** one thing, person, or group compared with another, usually in a way considered to be unfair.Bias -	Pair or group students before each activity to discuss the topic before opening it up to the whole class: ● What is bias? ● Example of bias ● Possible examples for our code. Challenge: How could we modify our code to be more truly M/L code?
	Look at the cipher code which "trains" the system.	**3**				
	Share the common issues with data in M/L by asking and showing examples.	**3**				
	Have students give possible data examples for cipher training in each case and try them.	**4**				
What next steps should we examine in M/L? (1 period)	Ted Talk "How to keep human bias out of AI" (12 m) https://www.ted.com/talks/kriti_sharma_how_to_keep_	**1**	This TED talk goes into more of a the general issues with M/L, big data and bias. Takeaway (from WMD slides): We are becoming increasingly reliant on predictive models and data. It is important that we take responsibility in regulating and integrating fairness into these models which dictate our data-driven society.	Movie: Coded Bias https://www.imdb.com/title/tt11394170/ Book: Weapons of Math Destruction https://www.programmer-books.com/weapons-of-math-destruction-pdf/ Slides summarizing Weapons of Math Destruction https://www.seas.upenn.edu/~cis399/files/lecture/presentations/Weapons_of_Math_Destruction.pdf	(same plus) **Intelligence**: Intelligence can generally be described as the ability to perceive or infer information, to be applied towards adaptive behaviors. **Artificia**l: Made or produced by human beings rather than occurring naturally. **Artificial Intelligence**: Intelligence demonstrated by machines. It keeps changing as machines become more capable. Any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. In Tesler's Theorem he says "AI is whatever hasn't been done yet." **Tesler's Theorem**: Tesler's Law of Conservation of Complexity (ca. 1984). "Every application has an inherent amount of irreducible complexity." http://www.nomodes.com/Larry_Tesler_Consulting/Adages_and_Coinages.html	Definitions of words which may otherwise seem obvious are useful not only for ELs but for the discussion in general. Graphic Organizers with key questions as a guide for research: What is AI? How does it relate to M/L? What things (sites, apps, etc.) which you use frequently use AI? Slides can be used instead of the book for summary and general ideas. Challenge: What should we make sure we do to make the best of the AI which is increasingly becoming common in our world?
	Discussion about M/L.	**2/3**				
	Mini-research and report.	**4**				
	Optional activity, HOC from code.org: "AI for Oceans" https://code.org/oceans (specifically in the last few steps you can see what characteristics the AI used for its pattern - which many times do not seem relevant to your choice)	**3**				

Instructional Supports				
Lowest 1/3 See differentiation suggestions.	**Highest ⅓** Extensions and/or Challenges	**SWDs** See differentiation suggestions.	**ELLs** Word Wall Re-use of academic vocabulary over several days, emphasizing use. Entry/Exit quizzes about vocabulary.	**Other**
Post Unit Reflection:				