UNIT 10: Cryptography

Estimated Time in Hours: 8

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 8 Implications	4.3, 8.1	- Practice various forms of symmetric cryptography using GUI interfaces and command line tools. - Paper-craft physical historical ciphers to reinforce concepts. - Decode Enigma machine messages in realistic scenarios.

Guiding Questions:

- How is information protected on the Internet?
- What is the process to turn plaintext into ciphertext?
- What is needed to decrypt a message?
- What are some common attacks against ciphers?
- What is the primary difference between symmetric and asymmetric cryptography?
- What are the two basic uses for asymmetric cryptography?
- How can you check Certificate Authorities used for web browsing?
- How has cryptography played a major role in warfare?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.3.1g EK: The primary goal of cryptography is to keep enciphered information secret.	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Ask students if they believe the Internet (social media, banking, gaming, e-commerce) is important to protect and whether they think it's safe. Ask how they believe things connected to the Internet are secured.
4.3.1 LO: Students will define cryptography and explain how it is used in data security.		• Introduce and define cryptography. You may give examples of secret writing or ask them to brainstorm how they would send a secret message.

4.3.1a EK: Cryptography comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning.		• Explain the difference between encryption and decryption. Emphasize the importance of encrypting information so adversaries cannot access it. • Affirm the question posed before: The Internet is protected by cryptography. • Explain how cryptography was important before the Internet and give examples of historical methods of encryption and their purpose.
4.3.1f EK: Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result.		• Explain the difference between plaintext and ciphertext. Use a before-and-after example from historical cryptography to show the difference. "You can plainly read the plaintext." • Introduce the term key as a requirement to change between plaintext and ciphertext.
4.3.1d EK: Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.		• Focus on the definition of encryption. Use a historical encryption example to the process of encryption.
4.3.1e EK: Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.	• "Cryptology STEM workshop 60-90 Mins." University of Colorado Colorado Springs Center for STEM Education, *UCCS.edu*,	• Emphasize the definition of decryption. Use the same historical example to show the process in reverse. • Task the students with building a historical cipher (e.g., scytale) and using it to encrypt and decrypt messages. Discuss any vulnerabilities in the chosen cipher.

	https://www.uccs.edu/Documents/pipes/cryptology-cdio.pdf • *AES Crypt*, https://www.aescrypt.com/ • *OpenPGP*, https://www.openpgp.org/	• Digital cryptography can be practiced on Windows or Linux machines using the provided AESCrypt and GPG resources. • Review the various cryptography terms they have learned so far.
4.3.2 LO: Students will practice symmetric cryptosystems to send a message and explain how they work.	• Sweigart, Al. "Cracking Codes with Python– Chapter 1: Making Paper Cryptography Tools." Invent with Python, *InventwithPython.com*, https://inventwithpython.com/hacking/chapter1.html • Sweigart, Al. "Cipherwheel." Invent with Python, *InventwithPython.com*, https://inventwithpython.com/cipherwheel/ • "Cryptography Worksheets– Worksheet 1: The Caesar Cipher." CS Unplugged for Middle	• Task students with practicing symmetric cryptography algorithms (e.g., Caesar cipher). Depending on skill level, they can create physical representations of the cipher, practice using online tools, or develop software to simulate the cipher. • Provide independent practice with cryptography using the provided csunplugged resource.

	Schools, Colorado School of Mines, *Mines.edu*, http://csunplugged.mines.edu/Activities/Cryptography/CryptographyWorksheets.pdf	
4.3.1b EK: Cryptanalysis is the breaking of codes. 4.3.2e: A shift cipher is susceptible to a statistical ciphertext-only attack.	• "Lesson Plans & Activities– Frequency Analysis Code Cracker." Spy Museum, *SpyMuseum.org*, https://spy-museum.s3.amazonaws.com/files/resources/code-cracker.pdf • "Caesar Cipher." dCode, *dcode.fr/en*, www.dcode.fr/caesar-cipher	• Provide examples of cryptanalysis. • Task students with cracking frequency analysis ciphers and exploring the feasibility of brute-force attacks. Tie this to the identifying strong vs weak ciphers.
4.3.1c EK: Cryptographic algorithms, also known as ciphers, are mathematical functions used in the process of encryption and decryption.		• Recap ciphers covered so far and introduce new ones. • Ask students why we have so many ciphers and how they think they have evolved over time.
4.3.2a EK: There are two basic types of symmetric ciphers: Transposition ciphers that diffuse		• Explain the difference between transposition and substitution ciphers

the data in the plaintext and substitution ciphers that replace the data in the plaintext. 4.3.2b EK: In transposition ciphers the letters are not changed they are rearranged. The set of encryption functions E is simply the set of permutations of m, and the set of decryption functions D is the set of inverse permutations. 4.3.2c EK: Anagramming is a way to attack a transposition cipher. It uses tables of n-gram frequencies to identify common n-grams.		• Show simple examples of how transposition would encrypt plaintext. Use historical ciphers as examples and ask students to identify whether they are transposition. • Discuss weaknesses of transposition ciphers. • Highlight the anagram attack and how it works. Have students spot commonly used anagrams in English.
4.3.2d EK: A substitution cipher changes characters in the plaintext to produce the ciphertext.		• Show simple examples of how substitution would encrypt plaintext. Ask students to identify historical ciphers that are substitution. • Ask what kind of techniques substitution ciphers are vulnerable to.
4.3.1h EK: Symmetric encryption is a method of encryption involving one key for encryption and decryption.		• Emphasize how symmetric cryptography must use the same key and list the ciphers you've covered so far that are symmetric. • Ask students what would happen if a symmetric cipher used a different key to decrypt.

4.3.1i EK: Public key encryption, which is asymmetric, is an encryption method that is widely used because of the enhanced security associated with its use.	• "Asymmetric encryption – Simply explained." *YouTube*, uploaded by Simply Explained, 30 Oct 2017, https://www.youtube.com/watch?v=AQDCe585Lnc&feature=emb_logo • "Prime Numbers & Public Key Cryptography." *YouTube*, uploaded by Simon Pampena, 2 Nov 2011, https://www.youtube.com/watch?v=56fa8Jz-FQQ	• Contrast asymmetric cryptography to symmetric. Emphasize how asymmetric means "not the same." • Show the video on asymmetric encryption and ask students review questions, including why two keys might be advantageous in some situations. • If the class is keen on how it is so secure, show the video on prime numbers in asymmetric cryptography. Consider creating a viewing guide to review how prime numbers are beneficial.
4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. 4.3.3b EK: Public key encryption uses a key pair - a private key known only to the entity and a cryptographically linked public key that can be shared with anyone.	• "Bitcoin: How Cryptocurrencies Work." *YouTube*, uploaded by SciShow, 21 Dec 2016, https://www.youtube.com/watch?v=kubGCSj5y3k	• Contrast private and public keys. Be sure students know which must be secret and which must be shared before proceeding. • Use graphics throughout the asymmetric cryptography sections. It is much more complex than symmetric. • Setup the "rules of asymmetric": if something is encrypted with one key, it must be decrypted with the other.

4.3.3a EK: Public key encryption does not require the sender and receiver to share the same key.		• If the class is advanced, consider introducing Bitcoin with the video.
4.3.3c EK: Secret messages encipher the message with the recipient's public key, are sent, and then the recipient can decipher it using their private key.		• Walk through an example of using asymmetric cryptography to keep messages secret. • Ask students how this is different than symmetric cryptography, and what advantages asymmetric may provide.
4.3.3d EK: Digital Signatures are a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.		• Walk through an example of using asymmetric cryptography to create digital signatures. • Ask students what are some uses of digital signatures. • Review these two methods before proceeding. Students should understand how asymmetric cryptography can be used two different ways to achieve different goals.
4.3.1k EK: Certificate authorities (CAs) issue digital certificates that validate the ownership.		• Demonstrate CAs in action by opening a web browser and navigating to a website. Click the details next to the URL to showcase the CA. Discuss web encryption and HTTPS.
8.1.1d EK: The loss of confidentiality is a critical factor in warfare.	• *Enigma M3*, https://www.101computing.net/enigma/ • Hinsley, Harry. "The Influence of ULTRA in the Second World War." 19 Oct 1993, http://www.cix.co.uk/~klockstone/hinsley.htm	• Practice hands-on decryption of realistic Enigma machine messages in the linked 101computing resource. • Emphasize cryptography's impact by explaining how breaking the Enigma codes shortened WW2 by 2-4 years.

8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		• Explore a relevant career, such as cyber defense forensics analyst.