UNIT 5: CRYPTOGRAPHY

Estimated Time in Hours: 16-17

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 4 Data Security 7 Risk 8 Implications	2.1, 4.3, 7.2, 8.1	- Scytale & Caesar Cipher - Caesar Cipher Program - Anagrams - Symmetric Ciphers - Steganography - Public Key Encryption & Digital Signatures - History & Politics of Public Key Encryption - Breakout Box

Guiding Questions:

- What are the ways in which data can be encrypted?
- What actions can be taken to validate that data has been unaltered by an unauthorized source?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
2.1.1 LO: Students will evaluate methods of keeping information secret from those whom the information should be kept secret EK: 2.1.1c,d 4.3.1 LO: Students will define cryptography and explain how it is used in data security. EK: 4.3.1a,b,c,d,e,f,g,h,i 4.3.2 LO: Students will practice symmetric cryptosystems to	• KWL Chart (find example KWL chart at https://www.timvandevall.com/templates/kwl-chart-template/) • "Cryptography: Crash Course Computer Science #33." *YouTube*, uploaded by CrashCourse, 25 Oct 2017, https://www.youtube.com/watch?v=jhXCTbFnK8o&feature=youtu.be • Cornell Notes	**Introduction to Cryptology: (1-day lesson)** This lesson introduces students to cryptography and the history of cryptography. • Students begin with a pre-assessment using a KWL chart to identify what they know about cryptography. Students then watch the Cryptography Video. Students take Cornell notes on the video. Once the video is over, students return to the KWL chart and add to it based on what they have learned and what questions they still have. The class discusses the purpose of encryption, and how it is necessary to ensure confidentiality and integrity. Students then gain hands-on experience with two types of encryption. They begin by creating a scytale. Students select a pipe and wrap the crepe paper around it. Using a

send a message and explain how they work. EK: 4.3.2a,b,d,e 4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. EK: 4.3.3a,b,c,d	(for an explanation of the Cornell note-taking system, visit http://lsc.cornell.edu/study-skills/cornell-note-taking-system/) • PVC Pipe (with varying diameters) • Crepe Paper, Ribbon, or Washi Tape • Markers • Caesar Cipher Wheel • Paper	marker, they then write a message on the crepe paper. Next, they unwrap the message and pass their crepe paper message to someone else in the class to solve. The person solving the message must have a pipe that is the same length and diameter. After this activity, students discuss the strengths and weaknesses of this form of encryption. Students then create a wheel for the Caesar Cipher. Students encrypt a message for another student in the classroom using the Caesar Cipher. The message is then passed to the other student to decrypt. After this activity students discuss the strengths and weaknesses of this form of encryption.
4.3.1 LO: Students will define cryptography and explain how it is used in data security. EK: 4.3.1d,e,f,g,h	• Python	**Caesar Cipher Program: (2-3-day lesson)** In this lesson students build a program to encrypt and decrypt information using a Caesar Cipher. • Using Python students write a program that will ask the end user if they want to encrypt or decrypt a message. If the end user wants to encrypt a message the program asks for the message to encrypt and the key. The program then encrypts the message and outputs it to the end user. If the user selects to decrypt the message, the program asks the user to enter the encrypted message. It then outputs the value of each shift and the possible decryption for each shift.
4.3.2 LO: Students will practice symmetric cryptosystems to send a message and explain how they work. EK: 4.3.2c	• "Anagram in The da Vinci Code." *YouTube*, uploaded by Idan Cohen, 19 Oct 2013,	**Anagrams: (1-day lesson)** In this lesson students learn what anagrams are and how they are a way to attack a transposition cipher. • This lesson begins with students watching the "Anagram in The da Vinci Code" video, followed by the clip from

	https://www.youtube.com/watch?v=OZj8bxV7x9I&feature=youtu.be • "The Da Vinci Code (3/8) Movie CLIP – So Dark the Con of Man (2006) HD." *YouTube*, uploaded by Movieclips, 25 Oct 2012, https://www.youtube.com/watch?v=F_HKGZRUroE&feature=youtu.be • "Anagram Solver." Word Tips, *Word.Tips*, https://word.tips/anagram-solver/ • Paper • Pen or Pencil	"The Da Vinci Code" movie. Students discuss what they saw in the two videos. Students go to the word tips webpage and read about anagrams. Students then create an anagram for another student in the classroom. The other student will solve the anagram. The class is wrapped up with a class discussion about anagrams.
4.3.2 LO: Students will practice symmetric cryptosystems to send a message and explain how they work. EK: 4.3.2a,b,d,e	• Notebook • "Rail-Fence Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/rail-fence/ • "Baconian Cipher." Practical Cryptography, *PracticalCryptography.com*,	**Symmetric Cryptosystems: (7-day lesson)** In this lesson students practice using different symmetric cryptosystems. • Day 1 - In this lesson students will learn about the Rail-Fence Cipher. Students receive an assignment that is encrypted using a Caesar Cipher. They have to solve the Caesar Cipher in order to find out what they need to do in the assignments. The assignment asks the students to read about the rail-fence cipher at the practical cryptography website. Students add an explanation about how the rail-fence cipher into their notebook. Students are asked to encrypt a message telling their

	http://practicalcryptography.com/ciphers/classical-era/baconian/ • "Polybius Square Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/polybius-square/ • "Vigenère and Gronsfeld Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/vigenere-gronsfeld-and-autokey/ • "Four-Square Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/four-square/	favorite class in school using the rail-fence cipher and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the rail-fence method. • Day 2 - In this lesson students will learn about the Baconian Cipher. Students will receive an assignment that is encrypted using the Rail-Fence Cipher. They have to solve the Rail-Fence Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Baconian Cipher. Students add an explanation about how the Baconian cipher into their notebook. It also assigns students into teams to play Mission Code X and assigns the students the number of missions they are required to complete. Students are asked to encrypt a message using the Baconian cipher that they must send to a student in another game team that tells how successful they were in completing the missions in Mission Code X. A student from another team decodes the message. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Baconian method. • Day 3 - In this lesson students will learn about the Polybius Square Cipher. Students will receive an assignment that is encrypted using the Baconian Cipher. They have to solve the Baconian Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Polybius Square Cipher. Students add an explanation about how the Polybius Square cipher into their notebook. Students

	• "Playfair Cipher." Practical Cryptography, *PracticalCryptography.com*, http://practicalcryptography.com/ciphers/classical-era/playfair/ • Neijts, Semilof, Clark, and Rouse. "steganography." TechTarget|SearchSecurity, *SearchSecurity.com*, https://searchsecurity.techtarget.com/definition/steganography#:~:text=Steganography%20is%20the%20technique%20of,for%20hiding%20or%20protecting%20data. • Online Steganography tool: "Steganography (encode text into image)." Many Tools, *ManyTools.org*, https://manytools.org/hacker-tools/steganography-encode-text-into-image/ • Paper	are asked to encrypt a message about their favorite unit so far in Cybersecurity using the Polybius Square cipher and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Polybius Square method. • Day 4 - In this lesson students will learn about the Vigenere Cipher. Students will receive an assignment that is encrypted using the Polybius Square Cipher. They have to solve the Polybius Square Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Vigenere Cipher. Students add an explanation about how the Vigenere cipher into their notebook. Students are broken up into groups and are asked to play the Crypto Go Card Game. Students are asked to encrypt a message using the Vigenere cipher about if they liked the game or not and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Vigenere method. • Day 5 - In this lesson students will learn about the Four-Square Cipher. Students will receive an assignment that is encrypted using the Vigenere Cipher. They have to solve the Vigenere Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Four-Square Cipher. Students add an explanation about how the Four-Square cipher into their notebook. Students are asked to encrypt a message about what cipher they like best using the Four-Square cipher and send it to another student to decode.

	• Pen or Pencil • Crypto Go Card Game: González-Tablas Ferreres, A. I. and González Vasco, M. I. (2018). **Crypto Go: Symmetric key - English (open source) [Card game]**. Madrid: Universidad Carlos III de Madrid, Universidad Rey Juan Carlos. Available at http://hdl.handle.net/10016/28433 • Mission X-Code, from Amigo Games (available for purchase on Amazon) • *Pico CTF*, https://picoctf.com/ • Abelson, Ledeen, and Lewis. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*. Addison-Wesley Professional, 2008.	The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Four-Square method. • Day 6 - In this lesson students will learn about the Playfair Cipher. Students will receive an assignment that is encrypted using the Four-Square Cipher. They have to solve the Four-Square Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about the Playfair Cipher. Students add an explanation about how the Playfair cipher into their notebook. Students are then asked to complete at least one puzzle the cryptography room in Pico CTF. Students are asked to encrypt a message about what they learned in the puzzle they completed in the cryptography room in Pico CTF using the Playfair cipher and send it to another student to decode. The students must turn in a copy of the encrypted message and the solution. Students then must decode someone else's message using the Playfair method. • Day 7 - In this lesson students will learn about Steganography. Students will receive an assignment that is encrypted using the Playfair Cipher. They have to solve the Playfair Cipher in order to find out what they need to do in the assignment. The assignment asks the students to read about Steganography in the Blown to Bits book - Hiding Information in Images (p. 95-99). Students add an explanation about Steganography into their notebook. Students are asked to encrypt a message in an image and send it to another student to decode. The students must turn in a copy of the encrypted message in the image and

		the plaintext. Students then must decode someone else's message hidden in an image.
4.3.1 LO: Students will define cryptography and explain how it is used in data security. EK: 4.3.1i,k 4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. EK: 4.3.3a,b,c,d 7.2.4 LO: Students will be able to explain how the decentralized and dynamic nature of networked systems create the potential for a system to fail or behave incorrectly due a component the designer didn't even know existed. EK: 7.2.4f,g,h	• Notebook • "The Internet: Encryption & Public Keys." *YouTube*, uploaded by Code.org, 21 Aug 2015, https://www.youtube.com/watch?v=ZghMPWGXexs&feature=youtu.be • "CS Principles 2017 | Unit 4 | Ch. 1 | Lesson 7: Public Key Cryptography | Activity 1 | Activity Guide – Public Key Bean Counting." *Code.org*, https://docs.google.com/document/d/1l0KDF33-gWIssZGqfuHgD0QpF50Pdyqras46FeuNLgc/edit • Modulo Widget • Public Key Crypto Widget • "The Story of Digital Signatures and Public Key Infrastructure." *YouTube*,	**Understanding Public Key Encryption and Digital Signatures: (2-day lesson)** In this lesson students gain a better understanding of public key encryption through hands-on experiences and learn about how public key encryption relates to digital signatures. • This lesson begins with students watching a video about Encryption and Public Keys. Students take notes on the video in their notebook. They then gain hands-on experience in how public key encryption works through the Cups & Beans Activity from Code.org. Once the students experience this, they discuss what they have learned from the activity. Students then work with the Modulo Widget to have a better understanding of the math behind public key encryption followed by using the Public Key Crypto Widget with a partner to gain hands-on experience with public / private key encryption. The class discusses the experience with the widget. Students then watch the video on Digital Signatures and take notes in their notebook. After the video there is a class discussion on how digital signatures relate to public and private key encryption. Students then update their notebooks with the key vocabulary.

	uploaded by PKIIndia, 29 Apr 2016, https://www.youtube.com/watch?v=G7hs-3R86M0&feature=youtu.be	
4.3.3 LO: Students will employ public key (asymmetric) encryption and explain how it works. EK: 4.3.3a,b,c,d 8.1.2 LO: Students will explain how the idea of the open internet led us to new innovations that impact our daily lives and our security. EK: 8.1.2c	• Window Notes Sheet (access a blank Window Notes template at https://toolsforclassroominstructionthatworks.com/wp-content/uploads/2018/01/Window-Notes.pdf) • "The Evolution of Public Key Cryptography." *YouTube*, uploaded by NYU Tandon School of Engineering, 23 Oct 2018, https://www.youtube.com/watch?v=Pk-Hqsjq5HU&feature=youtu.be • Abelson, Ledeen, and Lewis. *Blown to Bits: Your Life, Liberty, and Happiness After the Digital Explosion*. Addison-	**History & Politics of Public Key Encryption: (2-3-day lesson)** In this lesson students learn about the history of public key encryption and how government policies discouraged the use of encryption to build secure networks. • Students read p.165-193 in Blown to Bits. This reading includes topics such as Historical Cryptography and Lessons for the Internet Age. Students take window notes while reading. Following the reading, there is a class discussion about what students learned in the reading. Students then watch the video on the Evolution of Public Key Cryptography and take window notes. After the video the class discusses public key encryption and government policy. **Assessment:** *In groups of 3-4 students complete a breakout box using ciphers and steganography.*

	Wesley Professional, 2008.	