LESSON 2: SPY TOOLS OF THE TRADE: CRYPTOGRAPHY, CODES, AND CIPHERS

Overview

In this lesson, students will learn about cryptography, the practice of writing "secret" messages using codes and ciphers. In Part 1, they will work with and uncover the codes and ciphers in The Great Canadian Cryptography Laboratory on the Spies in the Shadows website. In Part 2, students investigate the history of cryptography by looking at, using, and creating their own codes and ciphers to send secret information. By the end of the lesson, students will have used and reviewed both historical and practical applications of cryptography.

Outcomes

Students will:

- analyze, synthesize, and record information
- identify historical and modern applications for cryptography
- gain an appreciation and knowledge of the uses of cryptography and ciphers
- use appropriate vocabulary
- examine the challenges of exchanging information in the absence of technology
- understand the importance of cryptology for security in the modern age
- formulate and answer questions
- communicate the results for specific purposes and audiences using different media, drawings, oral presentations

Duration

several class periods plus research time

Skills

writing, researching, communicating, critical thinking, interpreting and analyzing, organizing, summarizing, presenting, comparing and contrasting, drawing conclusions, using media communications

Materials

- paper, pens, pencils
- notebook paper
- *Spies in the Shadows'* website (The Great Canadian Cryptography Laboratory)
- BLM 1 Breaking the Codes (for Part A)
- BLM 2 The Great Canadian Cryptography Laboratory Answer Key (for Part A)

- BLM 3 Build Your Own Cipher Wheel (for Part B)
- BLM 4 Cryptography Research Questions (for Part B, Extensions)

Teacher Background and Notes

Cryptography literally means "secret writing," and is the official name for codes and ciphers. One of the main tasks of a spy is to exchange messages, while keeping the content of these messages secret to those who would intercept the message.

A code is specifically defined by a "code book," essentially a dictionary of substitutions from the plain text (alphabetic) to a coded text. Ciphers are what most people think of when they hear the term cryptography (e.g.: the Caesar cipher or the cipher wheel). Essentially, a code is a system in which every word or phrase in an original message is replaced by another word, phrase, or series of symbols. A cipher is a system in which every letter in an original message is replaced by another letter or symbol.

Throughout history, codes and ciphers have been written and broken by humans, concealing a plain text message by replacing or scrambling its letters through mathematical formulas or algorithms to encipher or decipher messages.

To be understood, a message has to follow a number of stages. An encoded message must be received by the recipient (or intercepted by an adversary), and written down exactly as sent. The encoded message must then be deciphered. If written in a foreign language, the message must also be translated. Then, an analyst must determine whether or not the information contained in the message needs a response. The final recipient must then determine what action is required.

While cryptography is often perceived to be closely linked to espionage, in practice it takes place everywhere, protecting commercially valuable information, war plans, romantic liaisons, and even building security. Some examples are listed below.

- Diplomats who send telegrams from foreign countries encrypt their messages so that the host country does not know what is being said about them.
- Credit card companies and banks encode financial transactions to ensure that private data owned by their clients is not easily read by others. These same companies also encrypt financial data for purchases made on the Internet.
- Many corporate e-mails between business partners are encrypted to ensure that information within them is not stolen by outsiders.

Part of the process of cryptography is to make the code or cipher difficult enough to render the message useless, or make it too much effort to decipher. For example, during a military campaign, knowing the location of armies is important, but understanding their intentions is even more crucial. However, information about an adversary's intentions is almost always time-sensitive. If one receives the information too late, the intelligence is useless. In such a case, the role of cryptography is to delay the decoding until the information no longer useful.

Teaching and Learning Strategies

Part A: The Great Canadian Cryptography Laboratory: Cracking the Codes

1. Tell students to go to the home page of the ***Spies in the Shadow's*** website, and click on the **Cryptography Laboratory**. **The Great Canadian Cryptography Laboratory** will appear on their computer screen. Before they begin the activity, suggest they read Canada and Cryptography on the site to provide them with a better understanding of codes and ciphers.

2. Pass out **BLM 1 Breaking the Codes**. Now divide the class into four groups. Each group will be assigned a specific cipher to explore as it appears on the desktop of The Great Canadian Cryptography Laboratory. The codes and ciphers are as follows:
    - book code cipher
    - secret ink cipher
    - Morse code
    - colour shielding cipher

3. Tell groups that they will be given a specific time to "crack the code" of their cipher. After that time, the group will then move to the next cipher based on the bulleted list in Step 2. By the end of the activity, all groups will have had an opportunity to open all four ciphers on the desktop.

4. To find their cipher, members in the group will hover their mouse over the desktop until a pop-up window appears with their assigned cipher. Another click and a window appears that provides students with a brief description and background on the cipher. From there, students will proceed to break the code of their ciphers. Suggest they write the answers in the chart on **BLM 1 Breaking the Codes**.

5. Pass out the **BLM 2 The Great Canadian Cryptography Laboratory Answer Key** to the groups. Have each group compare their deciphered messages on the BLM to those on the Answer Key. Which messages are similar, and which are different? Tell students to make the appropriate adjustments on their BLM.

6. Then, as a class, discuss the advantages and disadvantages of each type of code and cipher. Ask students to determine under what circumstances one might be better than another. What conclusions can they make about the complexities of passing and cracking "secret" messages using different methods of ciphers and codes?

Part B: Cryptography History: Codes and Ciphers

13. Tell students that in this activity they will investigate the history of cryptography—the art of secret message writing using a code and cipher. Ask them to speculate what the difference is between a code and cipher. (**Note***:* Some students who play online or video games, read espionage or science fiction novels or non-fiction, or watch spy movies or television series may be familiar with these two words. Others in the classroom may need more help in understanding the differences between these two words.)

14. Write out their responses on the chalkboard in a T-chart in which the word "code" is written on one side and "cipher" on the other. Review the T-chart with students and ask them to come to some consensus about which response best describes the difference between code and cipher. (**Hint:** A code is a system in which every word or phrase in an original message is replaced by another word, phrase, or series of symbols. A cipher is a system in which every letter in an original message is replaced by another letter or symbol.)

15. Mention to students that codes and ciphers have been used by humans to secretly communicate with each other throughout history. One example was used by the Roman Emperor Julius Caesar (100-44 BCE) to communicate to his generals. Eventually referred to as the Caesar cipher, this simple alphabetic substitution system shifts the alphabet three places so that

    ABCDEFGHIJKLMNOPQRSTUVWXYZ

    now becomes

    XYZABCDEFGHIJKLMNOPQRSTUVW

16. Write this message on the chalkboard: JBBW FK ZIXPP. Now ask students to decipher it. The deciphered message is MEET IN CLASS. Ask students how difficult or easy it was to break this code.

11. Mention to students that Italian architect Leon Alberti in the 15th century invented another cipher called the cipher wheel or disk. This cipher disk follows some of the same principles as the Caesar cipher (shifting of the alphabet to create and decipher a message). In this case, two disks are used to produce and break the coded message.

12. Pass out the **BLM 3 Build Your Own Cipher Whee**l. Tell students that they will work in pairs to create their own cipher wheel based on the instructions in the BLM.

13. Ask a few pairs to volunteer their answers to the class. How successful were their efforts to create and decipher their codes using the cipher wheel? What have students learned so far about the passing of information using a basic cryptography method?

Extensions

14. Now that students have looked at and used some basic codes and ciphers, invite them to investigate and examine some more complex types of cryptography tools. Suggest they research why the following tools were developed and how they changed history. Invite them to choose one of the following ciphers:
    - Enigma machine
    - Purple cipher
    - Rockex cryptosystem
    - Venona decrypts
    - Arnold cipher
    - Semaphore

    Encourage students to decide on the best way to present this information to the class. Examples are as slide or PowerPoint presentation, oral report, photo essay or collage, timeline, or "secret" document or dossier to name few.

15. In small groups, suggest that students list popular books, television shows, or movies that demonstrate codes and ciphers. Some examples might include Sherlock Holmes or Harry Potter novels; television shows like *Numbers* or *24;* movies such as *Sneakers*, *National Treasure, Windtalkers*, *The Da Vinci Code, or* the *Harry Potter* series. Invite students to describe the type of cipher or cryptology used by listing it in point form in their notebooks.

16. Today the development of computers and electronics has led to the use of more complex cryptography by governments and corporations. Personal lives are also affected by this type of cryptography that prevents fraud and identity theft, but also invades privacy. Have students consider the number of ways in which they use a form of cryptography on a daily basis such as a code or password to access or send messages and make transactions. Some examples are listed below.
    - Using ATM or credit cards to conduct electronic commerce or to take out books and other resources from a school or public library
    - Scanning bar codes to make purchases at stores or online using a smartphone
    - Logging on to a social media site or a computer
    - Texting messages to friends and family using a cell phone

    Invite students to keep a three-day log in which they make note of every time they use some form of cryptography such as those listed above. Suggest they share this information with another student. How often did they use a code or password to access or send messages? Why was this encryption important for them to conduct personal or business transactions? What does this say about the use of cryptography in their lives?

17. Language is itself a code. During World War II (WWII), Navajo code-talkers from the US communicated messages during most battles in the Pacific during WWII. Due of the success of this code breaking, the US Air Force stationed in Britain requested that Aboriginal soldiers from Canada encrypt and decrypt messages about bombing missions that involved Germany. A number of Cree soldiers assisted in this operation. Describe why Aboriginal languages would be a different way to send coded messages during WWII, and discuss other examples of linguistic cryptography. Suggest that students look up some information about Aboriginal code-talkers on this site: http://www.veterans.gc.ca/eng/sub.cfm?source=feature/week2001/media01/cree

18. At sporting events, coaches and players use hand signals to share information with their own players and keep it secret from the other team. The use of flags in naval communications (a semaphore) to communicate with each other is another type of cryptography. Ask students why it is important for coaches and players to use hand signals in playing sports, or for naval personnel on ships to communicate in this way? Do students think that hand signals might be used in espionage to protect or pass information to others? Explain.

19. As a concluding activity, pass out **BLM 4 Cryptography Research Questions**. Suggest that students add their responses to the questions. Then ask students to think about the use of cryptography in collecting secret information. Is intelligence gathering using codes and ciphers always accurate? Why or why not?