Lesson Plan: The Secrets of Cryptology – Cracking the Caesar Cipher

Materials Needed

- Pencils, Pens, or Markers
- Paper (Lined and Plain)
- Rulers or Compasses (optional, for making the cipher wheel neat)
- Scissors and Brass Fasteners/Brads (to construct the wheel)
- Printout: Caesar Cipher Wheel Templates (two concentric circles) or scrap cardboard for construction
- Handout/Digital Display: The alphabet written 1-26 (A=1, Z=26)

I. Introduction: The Art of Secrecy (15 Minutes)

A. Hook: The Uncrackable Command

Educator Prompt: Imagine you are a military general 2,000 years ago, and you need to send a crucial battle plan to your troops 100 miles away. If the enemy captures the messenger, they win the war. How do you guarantee the message can only be read by the intended recipient? Can you create a message that looks like nonsense but holds a powerful secret?

(Allow time for discussion/brainstorming on methods of secrecy, like hidden ink or complex language.)

B. Learning Objectives (Success Criteria)

By the end of this lesson, you will be able to:

1. Identify the difference between plain text (readable) and cipher text (coded).
2. Explain how a substitution cipher, specifically the Caesar Cipher, works using a "shift" key.
3. Successfully encode and decode short messages using a specific key (shift number).

Success Criteria: You will know you are successful when you can create a coded message and your partner (or the educator) can decode it back to the original meaning using only the key you provide.

II. Building the Cryptosystem (45 Minutes)

A. I DO: Modeling the Basics (15 Minutes)

Concept Introduction: Plain Text vs. Cipher Text

- **Plain Text:** The original, readable message (e.g., ATTACK AT DAWN).
- **Cipher Text:** The scrambled, unreadable message (e.g., DWWDEN DW GDAQ).
- **Key:** The secret number or word needed to unlock the cipher (e.g., Shift 3).

Modeling the Caesar Cipher (Substitution)

Educator Demonstration: The Caesar Cipher is named after Julius Caesar, who used it to communicate with his generals. It is a simple shift cipher. Every letter in the plain text is replaced by a letter some fixed number of positions down the alphabet.

Example Modeling: Let's use a Key of 3 (Shift +3).

If the plain text letter is **A**, we shift 3 places: A → B → C → **D**.

If the plain text letter is **T**, we shift 3 places: T → U → V → **W**.

I will encode the word 'CODE':

- C + 3 = F
- O + 3 = R
- D + 3 = G
- E + 3 = H
- Cipher Text: FRGH

B. WE DO: Constructing and Applying the Cipher Wheel (20 Minutes)

Activity 1: Cipher Wheel Construction (Kinesthetic/Visual)

1. Learners cut out two concentric circles (or draw them). The inner circle should be slightly smaller and fit inside the outer one.
2. Write the alphabet (A–Z) around the outside of the larger wheel.
3. Write the alphabet (A–Z) around the inner wheel, making sure the letters align initially.
4. Attach the center of the wheels with a brad or fastener so the inner wheel can rotate freely.

Transition: Now we have a tool that lets us instantly apply any 'shift' key!

Activity 2: Decoding Practice

Educator provides Cipher Text and Key:

- **Cipher Text:** YJSI
- **Key:** Shift 2 (or set the wheel so the outer A aligns with the inner C)

(Learner uses the wheel to decode, focusing on working backward. If A=C, then C must equal A when decoding.)

Feedback/Formative Assessment: Check the resulting word (Motto: "SEEK"). If correct, proceed.

C. YOU DO: Independent Encryption (10 Minutes)

Activity 3: Secret Message Exchange

Cherai must choose a secret Key (1 through 25). The learner then writes a short (5-10 word) command or message related to a favorite hobby or game (e.g., "Find the hidden gold in the dungeon," "Level up before the next match").

1. **Encode:** Use the chosen key and the cipher wheel to convert the Plain Text into Cipher Text.
2. **Transmit:** Give the educator (or designated recipient in a group setting) the Cipher Text and the Key.
3. **Decode:** The recipient must successfully decode the message back to the original Plain Text.

Self-Correction/Reflection: If the message is decoded incorrectly, the learner must trace the encoding steps to find the error (Did they skip a letter? Did they apply the shift consistently?).

III. Conclusion and Application (10 Minutes)

A. Recap and Real-World Relevance

Review Questions (Learner Recaps):

- What is the most important piece of information you need to decode a simple substitution cipher? (The Key/Shift number)
- Why did ciphers like this eventually stop being used for serious military communication? (They are too easy to crack—there are only 25 possible keys.)

Application: Discuss how cryptology is essential today, moving from military messages to digital security (passwords, encryption of online transactions, secure messaging apps). Even though the Caesar Cipher is simple, it is the foundation of modern cybersecurity.

B. Summative Assessment and Feedback

The successful completion of the "YOU DO" activity (creating and solving the secret message) serves as the primary assessment of objectives 2 and 3.

Feedback: Provide specific feedback on the accuracy of the shift and the clarity of the presentation of the cipher text.

C. Differentiation and Extension Challenge

Scaffolding (For initial difficulty):

- Provide a pre-solved message chart for the first practice run instead of requiring independent wheel construction.
- Focus only on letters A-M for the first few examples to avoid wrapping around the alphabet.

Extension (For advanced learners/Cherai):

The Cryptanalysis Challenge: Frequency Analysis

Challenge the learner to decode a Caesar Cipher message *without* being given the key. Provide a longer cipher text (30-40 words).

Instruction: English text has predictable letter frequencies (E is the most common letter). Count the letters in the cipher text. Assume the most frequent letter in your cipher text corresponds to 'E' in plain text. Use this discovery to find the shift key and decode the rest of the message. This introduces the concept of cryptanalysis (code breaking).