

---

# *Cryptography*

Lou Hodgson, Hannah Jeffers, Briana Bonsu,  
Will Gillette, Alan Okinaka

# Guiding Questions

---



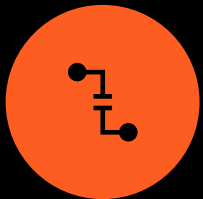
What is cryptography, and why does society use it?



How can corporations and businesses use cryptography to secure classified information?



How does the Caesar Cipher method encode information? What are the benefits and costs of using it?



How does the Random Substitution method work to encrypt data? How does it compare to the Caesar Cipher method?



How can individuals examine character frequencies as a tool for decryption?

# *What is Cryptography?*

---

- Cryptography: The process of encoding information so that only exclusive people or groups can decipher the information.
- Cryptographic Methods:
  - Caesar Cipher
  - Random Substitution
  - Vigenère Cipher
- Examples where cryptography is used:
  - Paid Television
  - Social media direct messages
  - E-money
- Activity:
  - Can you think of any other examples?

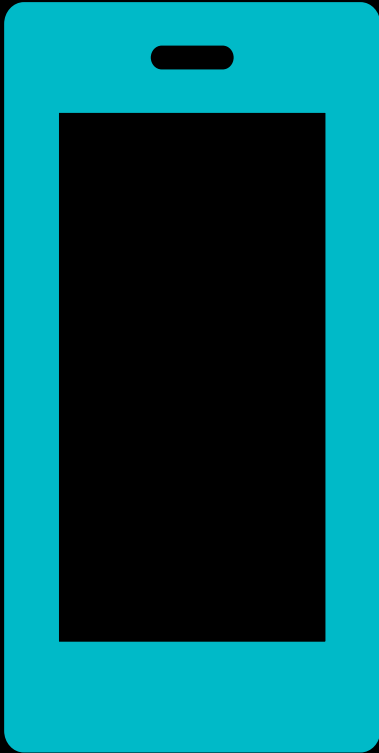
# *Widget Exploration Activity*

---

- Visit [CS Principles Widgets | Code.org](#), and navigate to the Cryptography widgets, opening both.
- Using the Cipher widget, decode this question and answer it. **Key=PASSWORD**
  - **SORPJHQNBONRWAOCITNUTCJLCNRD\_GYRSS?**
- The message below was encoded using the Ceasar cipher method with a shift of 7 characters. Using the [Frequency analysis widget](#), decode this one.
  - **Ghp, xgvhwx mabl fxlltzz nlbgz max ktgwhf lnulmbmnmbhg, tgw kxihkm rhnk kxlnem.**

# *Central Takeaways*

---



## Students will understand:

- That cryptography is the process of encoding information so that only exclusive people or groups can decipher it and has many applications in the technical world.
- That the Caesar cipher cryptographic method involves shifting the English alphabet by a certain increment to purposefully shuffle the characters in a message. The message can be easily decrypted because there are only 26 letters in the English alphabet.
- That the random substitution cryptographic method involves arbitrarily shuffling the characters of the English alphabet. Using this method makes it significantly more challenging for external parties to decrypt messages compared to the Caesar cipher because the resulting alphabet is not in any specific order.