

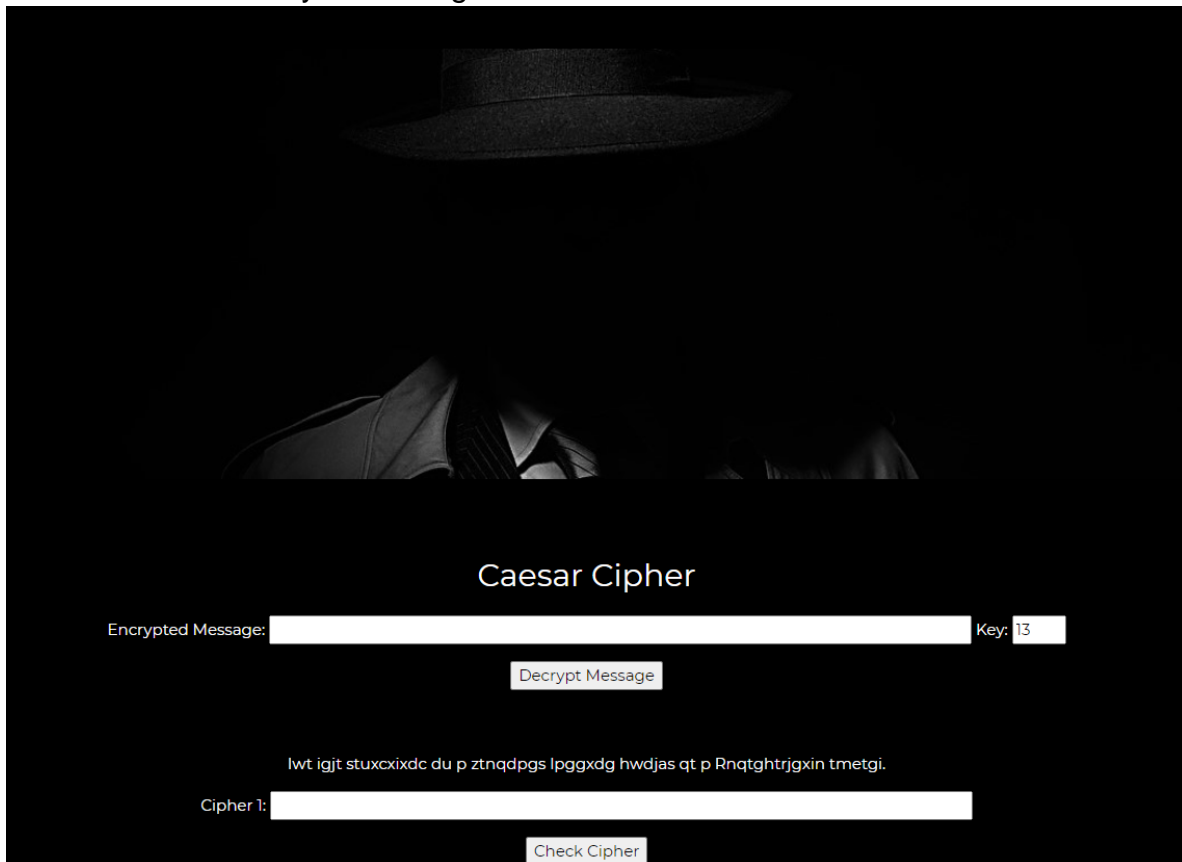
Johnny Cipher Teacher Workout Instructions

Introduction

This workout will introduce students to basic key cryptography with the ever popular Caesar cipher. Here is a Wikipedia article that gives the basic overview on how the encryption and decryption process works for a Caesar cipher.

The Workout

This workout is pretty straight forward. Students will be given a random combination of three ciphers that were encrypted using the Caesar cipher and they must see if they can decrypt the cipher either by hand or by using the tool provided on JohnnyHash. Students should avoid just guessing. Instead, they should use frequency analysis or word length to try and find the key. They should be able to find the key in 1 or 2 guesses.



The screenshot shows the JohnnyHash Caesar Cipher tool interface. At the top, there is a dark image of a person wearing a wide-brimmed hat. Below the image, the title "Caesar Cipher" is centered. The interface includes two main input sections. The first section is labeled "Encrypted Message:" and has a long text input field. To the right of this field is a "Key:" label followed by a small input field containing the number "13". Below these inputs is a button labeled "Decrypt Message". The second section is labeled "Cipher 1:" and has a long text input field. Below this field is a button labeled "Check Cipher". In the center of the interface, between the two input sections, is a line of encrypted text: "lwt igjt stuxcixdc du p ztnqdpqs lpggxdg hwdjas qt p Rnqtghtrjxin tmetgi."

If a submitted guess is correct, the input box will turn green. Once students have correctly decrypted all three messages, the workout will automatically be marked as complete!

Reflection Questions

Q1: What techniques were effective in finding out the key?

A1: Either frequency analysis or word length analysis

Q2: Match the following element to its corresponding cryptographic building block:

PBZRFOQB Ciphertext

SECURITY Plaintext

3 Key

$c_i = p_i + 3 \pmod{26}$ for each p_i in $P \rightarrow E_K(P)$

$p_i = c_i + 23 \pmod{26}$ for each c_i in $C \rightarrow D_K(C)$

Q3: A Caesar Cipher is a type of substitution cipher in which plaintext characters are substituted for the corresponding ciphertext. If you obtained the following encrypted message, how would you know it was a substitution cipher? fexs bxpz zobq clov lrfc vlrz xkjb bqjb xqax tk

A3: By frequency analysis, you can determine the ciphertext has a pattern similar to the English language in the frequency of each symbol.