Both the Caesar Cypher and the Polyalphabetic Cypher are viable options for encoding a message, but the Caesar Cypher suffers a much larger flaw than the Polyalphabetic Cypher. The Caesar Cypher has one layer of protection. All of the letters within the cipher are shifted a certain number of letters back; if encrypting the message “Zelda” with a one-letter back Caesar Cypher, it would become “Ydkcz.” This seems like gibberish, but it can be easily deciphered by simply being moved one letter forward. Any Caesar Cypher can theoretically be solved by shifting every letter 26 different times, giving all possible answers. Most likely, only one will make sense. The Polyalphabetic Cypher has multiple layers of protection. First, a codeword is decided that changes how many letters forward each letter of the actual message goes (i.e. the codeword ABCD would change the first letter 1 forward, second letter 2, third 3, fourth 4). This codeword is then implemented for every letter in the message (Lana Del Rey would go ABCD ABC DAB). So to figure out the message, the codeword also has to be figured out. This is much harder to do than a Caesar Cypher, as there are an infinite number of words to use in a Polyalphabetic Cypher, but only 26 different letters to use in a Caesar Cypher.