***Solution Explanation:*** Caesar Cipher

In order to solve this problem, it’s helpful to think about the order that the letter shifts along the given key. Let's think about the basic key which concludes all the capital letters (ABCDEF…XYZ) as an example. If the message is ABA and the shift is 3, it means from A, it moves from the original letter to the right by 3 so we have the new message as DED. However, the prem states that we need to find the original message with the given decrypted string. So, we need to reverse the formula to find the original message. For example, if the shift is 3, now we need to shift the character in the string to the left in order to find the original message. Since we have the basic idea of the cipher, we have a general formula to solve the problem: DK(I) = (I-k) mod N where N is the length of the given string, I is the position of the character in the string, and k is the shift of the character.

For example, the given key is ABCDEFGHIJKLMNOPQRSTUVWXYZ and the shift is 3.

|  |  |  |  |
| --- | --- | --- | --- |
| Encrypted Message | D | E | D |
| I | 4 | 5 | 4 |
| I-k | 1 | 2 | 1 |
| Decrypted Message | A | B | A |