According to the assignment given to us by OCRAI, our task was to successfully construct a system in which we could encrypt text messages. One of the most important aspects of the system was to have a set method and flexible/interchangeable keys that can allow employees to successfully communicate using a secure method. We have provided a means to accomplish this.

In order to create the key, we first listed all the letters of the alphabet in alphabetical order, then listed the punctuation that our message required, which, for our messages, included period, exclamation point, question mark, comma, and apostrophe. This gave us a total of 31 characters in our key. We assigned those punctuation marks a number 27 through 31.

Our method requires a shift in the order of the characters we use. In order to achieve this, an equation must be created to indicate where the shift begins in the key, and this equation is then put at the beginning of the encrypted message. (This allows for multiple keys to be created using the same method, because the sender can create any equation.) Once the receiver gets the message and solves the equation, they can begin creating the key that will decrypt the message.

Once the letters of the alphabet are put in alphabetical order, followed by the necessary punctuation marks, the solution to the equation will indicate where to start. We decided that if
the solution was positive, we would start from A and count down the characters until you reach the number that corresponds to the solution. If the solution is greater than the number of characters you have, you just begin at A again and continue counting. If the solution is negative, we decided to start at the last character and count up the characters until we reached the number that corresponds to the solution. If the solution is greater than the number of characters, you just begin at the last character and continue counting.

Once we reached the corresponding character, we decided to re-label all the characters, assigning A to that corresponding character, and continuing through all the characters, moving in the same direction we did in counting. When we reached Z in our re-labeling, we continued with numbers, starting with 1. (There should be a one-to-one correspondence between the ciphertext and the plaintext.) From there, we took our plaintext message and replaced every character with its re-labeled corresponding character. This new message is the ciphertext.

In order to decrypt a message that has been encrypted in this manner, we would need to follow a similar procedure, solving the equation to find the starting point, and re-labeling the characters to create a key for the ciphertext. From there, we would be able to decrypt the message through letter replacement.

This method of encryption allows for security in communication and enough variability to make it difficult for outside parties to listen in. The one-to-one correspondence, as well as the use of familiar symbols, allows for messages to be sent easily via text messages. Also, the simplicity of the math used allows for the majority (if not all) of your employees to be capable of using this method. Thus, this is a perfect solution to help avoid the several recent major security breaches.