The assignment we have been given is that of creating a method of encryption enabling someone to encrypt a text message to another person in a manner that would no more than quadruple the original length of the plain text. Using a key, the plaintext would be encrypted, protecting it from interception until it safely arrived in the hands of the desired recipient, who would then decrypt the message back into its original form.

The text messaging requirement limited our options in a few helpful ways. The first was that our encryption method had to be fairly easy to use, and had to only use either numbers or letters - we elected to use both. The second was that our key could no more than quadruple the plaintext. We associated each of the letters with a number according to its place in the alphabet; A=1, B=2, …etc. Next we selected a key word to be used to encrypt our message. Once we select the key word, say for example purposes the key word is BIG, we used each participating letter’s number to build the key. Using our hypothetical key word BIG, our key number would be 2-9-7. In order to encrypt a message, one must multiply the first letter by the first number in the key, the second letter in the word by the second number in the key, and so forth, repeating the key as many times as is needed. This method also required that we find a way to deal with the spaces and periods. The original idea was to simply leave the spaces and periods in their original plaintext format such as the one we decoded in class, but soon decided we wanted it to be less obvious, making it harder to crack. We began by multiplying the largest number in our key by the largest number in the alphabet, Z which is 26, to find out what the highest possible number our code could produce would be. We had to be sure not to choose a number that could be potentially produced by our key and a letter. This maximum integer is 546, so we chose
something in the 900s to safely evade any overlap in the code. However a number in the 900s
would be easy to pick out and would make it easy for Eve to identify these two numbers as the
punctuation and space, so this method was scratched as well. Next we decided on prime
numbers, but again ruled them out as being too easy to identify. Our final choice was 27 for
periods and 28 for spaces that are also multiplied by the key to produce the numerical value, so
they would be hard for someone to pick out as being distinctly different from the rest. The next
issue was that of distinguishing a letter from the next letter once the message had been encrypted.
We decided that since the maximum coded letter produced was three numbers long, we would
just make all the letters three numbers long, adding zeros if it failed to meet the three number
requirement. For example, if the number produced was 36, it would become 036 for purposes of
the code. This way all the numbers could be squished together, making it nearly impossible for
Eve to break it into words and sentences. Our method also prevented double letters from being
easily identifiable, since each of the double letters would be multiplied by a different key number
and would thus produce different numbers. As an example of how our encryption method is
used, let’s select BIG as our key, giving us 2-9-7. If the plaintext word were APPLE, using our
key we would multiply 2*1,9*16,7*16,2*12,9*5. After multiplying it out we get 2 144 112 24
45. Adding the zeros we get 2144112024045 which is the encrypted word. In order to decrypt it,
you would segment it into sets of three integers, divide each set of three by the appropriate
number from the key and translate it back into letters.

The solution to our problem was that we would use both letters and numbers to encrypt
the plain text message. The key word produces a numerical key that is then multiplied by the
number of the place the letter holds in the alphabet. This produces a three digit integer that
signifies that letter in the encrypted message.
This method produces an encrypted message that no more than triples the original length of the plaintext, can be easily incorporated into several text messages, and would be complicated to decode if the key was not available. Thus we accomplished all of our goals using this method of encryption.