

**TO:** OCRAI Board of Directors

**DATE:** 11 September 2015

**SUBJECT:** Project 4

## **INTRODUCTION:**

OCRAI has recently experienced many security breaches due to text messages received by unintended recipients. The texts contained important company information that needs to remain confidential, such as trade secrets. Fortunately, none of this classified information was disclosed to the media or our competitors. Had such a thing occurred, the company would have experienced much embarrassment and potential harm. In order to prevent such a catastrophe from arising, OCRAI has contracted with us to devise a method for keeping all correspondence within the company secure.

## **PARAMETERS:**

In order to make the encryption and decryption methods compatible with text messaging the following parameters must hold within our method:

- ⑩ It must take a text message of up to 140 characters (characters in 1 standard text message) and output a text message of up to 700 characters (characters in 5 standard text messages).
- ⑩ It must have an encryption key less than or equal to 10 letters long.
- ⑩ It must only contain symbols compatible with standard keyboards.

## **METHOD**

We have developed an encryption method in order to manipulate the plaintext of a message such that those desiring to intercept the message will be unable to read it. The encryption method operates as follows:

1. The application counts the letters in each word. (ex: cow = 3)
2. Each letter in the word is shifted forward by the number yielded in step 1. (ex: cow >> frz)  
(note: If the end of the alphabet is reached, return to the beginning. tax >> wda)
3. Following this shift, the entire message is then shifted again by a random positive integer. This step is the encryption key. (ex: If key = 5, cow >> frz >> kwe)
4. The recipient's application will then decrypt the ciphertext message.

In order to decrypt the message, the encryption method is reversed. For example, if the key = 3, then shift each letter in the ciphertext back 3 steps in the alphabet. Following that, count the number of letters in each word and perform step 2 above with shifting the letters backward in the alphabet instead of forward.

With such a dynamic encryption method that changes with each word, the safety of OCRAI's communication and intellectual property is ensured.

## **CONCLUSION:**

The protection of sensitive data and information is essential for the well-being of a business. The cipher we have created involves shifting each letter according to the length of each word and then shifting the entire alphabet depending on the encryption key. Through the use of this encryption method, OCRAI's confidential information will remain secure and the business will be protected from potential embarrassment and harm.