Group A

[redacted]

Math 485
Project 4
September 11, 2015

OCRAI Technical Report

In response to recent security breaches, OCRAI has asked that we create a nontrivial method of encryption to keep company information secure. Because the security breaches have occurred when company employees have accidentally sent text messages to the wrong recipient, OCRAI has asked that our encryption system be capable of encrypting a plaintext message of up to 140 characters in length (the length of a standard text message) and outputting a ciphertext that can be sent in, at most, 700 characters (the length of five text messages). The user must be able to input the message in standard characters.

As a result, we have created an algorithm that converts each letter into a three-digit number. To do so, we begin by randomly choosing a letter to be assigned the value of 1. The next letter in the alphabet is assigned the value of 2; the next, 3. This continues throughout the alphabet until each letter has been assigned a numeric value. We then choose any three-digit number between 000 and 999 that is equivalent to that letter's value, mod 26. This three-digit number is the ciphertext translation of the plaintext letter. We then take each letter of the outgoing message and convert the letter into its three-digit ciphertext equivalent. The three-digit numbers are written one after the other, not separated by spaces, periods, or other marks. Because of this, punctuation marks may be included or left out, as desired.

However, the space character is replaced by a period followed by a space (‘. ‘) in order to more clearly show the beginning and ends of words.

As an example, suppose we assign the letter *D* a value of 1, *E* a value of 2, and so forth. Then we can choose any three-digit number equivalent to 1 (mod 26) to represent *D*, any three-digit number equivalent to 2 (mod 26) to represent *E*, etc. For instance, we might choose 027, 391, or 625 to represent *D*, and 080, 184, or 730 to represent *E*. By following this pattern, we could represent the alphabet as follows:

Letter	A	B	C	D	E	F	G
Numeric Value	24	25	26	1	2	3	4
Ciphertext	596	805	000	391	730	523	394

This encryption system creates roughly 1.53×10^{55} different ciphers. There are 26 ways to shift the alphabet (i.e., to assign a numeric value to each consecutive letter of the alphabet). Because there are approximately 38 different values between 000 and 999 for each numeric value (mod 26), we can assign one of these 38 three-digit cipher-values to each letter. Therefore, with 26 shifts of the alphabet, and 38 different ways to represent each of the 26 letters, there are a total of 26 x (26^38) ways to encrypt the alphabet, or 1.53×10^{55} different ciphers. While this encryption algorithm creates more than a septendecillion ciphers, the receiver can relatively easily decrypt the messages once they have the key.

The sender must begin each message with the key words “I am”. According to the alphabet shift listed above (with *D* equal to 1, etc.), “I am” could be encrypted as

"162. 596790". From this key, the receiver can take the first value (mod 26) and see that $162 \equiv 6 \pmod{26}$, and therefore the letter *I* is assigned the numeric value of 6. The receiver may then number the rest of the alphabet—*J* would be assigned the numeric value of 7, etc. He or she will then find the value (mod 26) of each three-digit "letter" throughout the message. By matching this value with its associated letter according to the alphabet shift indicated by the key, the receiver can fully decrypt the message.

This algorithm allows us to encrypt any text messages exchanged between company employees. Moreover, because each plaintext character is replaced only by three ciphertext characters (with exception of the space character, which is replaced only by two characters), the maximum message length would be 420 characters, well within the limit requested by OCRAI. In accordance with OCRAI's desires that such information leaks not happen again, we are confident that this encryption algorithm will provide increased security to the company.