Group I

IMC

IMC Independent Mathematical Contractors, Inc.

136 TMCB

Provo, UT 84602

---

11 September 2015

OCRA Creative Recursive Acronyms, Inc.

485 Primality Way

Provo, UT 84604

Dear OCRAI:

We received your letter concerning your request for a method of preventing security breaches of text messages sent by your employees. We have put together a method for encrypting plaintext English messages that we believe will protect the security and confidentiality of your company's information. Included in this report is a description of the method for encrypting messages, a description of the method for choosing an encryption key, and three sample ciphertexts encrypted using the method described with three different encryption keys.

Our method of encryption randomly assigns three two-digit numbers to each of the characters letters A through Z (not case-sensitive), space, period, comma, and question mark, for a total of 30 characters. (Any numbers communicated through the method must be spelled out.) To choose the encryption key, we first assign three two-digit numbers from 00-89 to each of the 30 plaintext characters. This should be done randomly either by hand, with a random number generator, or with a computer program we have created which is also available for purchase. Once the encryption key is chosen, we substitute each character in the plaintext with one of the three corresponding two-digit ciphertext numbers. This is done randomly by hand or with a random number generator. The plaintext is then properly encrypted and the ciphertext is ready to be sent. The resulting ciphertext should appear as a string of numbers without spaces.

For example, say we wish to encrypt the message "Robert S. Andrews" using this method. Our program generates the following encryption key:

Plaintext → Ciphertext
A → 00, 30, 60
B → 01, 31, 61
D → 03, 33, 63
E → 04, 34, 64
N → 15, 45, 75

O → 16, 46, 76
R → 18, 48, 78
S → 19, 49, 79
T → 20, 50, 80
W → 23, 53, 83
Space → 26, 56, 86
Period → 28, 58, 88

After replacing each plaintext character with a ciphertext number (randomly chosen of the three), the ciphertext could appear

"48166104188026795856004533784623 19" or "18760134782056198886301503485379"

depending on which of the three two-digit ciphertext numbers is chosen for each plaintext character.

We believe that this method will secure communication over employees' mobile phones. We have decided on this method because it is more secure than a simple shift cipher. There are three numbers for each letter, making it difficult to discover all the possible numbers that represent a certain letter. Furthermore, the numbers that are chosen do not have to be in any order. For example, A → 1, B → 2, etc. The numbers assigned are random with no pattern that is easily discovered. Finally, space also has numbers associated with it, meaning that a person cannot use spaces to find where words end and begin, which would make the ciphertext easier to decrypt.

Yours sincerely,

[redacted]