Group J

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 inquiry about a solution to your security breaches. We recognize that the problem was that company employees were unintentionally and erroneously sending text messages – which contained sensitive company information and trade secrets – to the wrong recipients. We also recognize the potential for this to cause acute embarrassment to the company and to harm future revenue streams if received by the wrong person. We have faced the problem of making sure that sensitive information sent out to employees through text messages is secure and protected. This is why we have created a special cipher that would be easy to implement as well as painless to understand for less cipher-savvy workers. This cryptosystem can be used to create a mobile application which will encrypt all text messages before being sent and decrypt any messages received from other company employees as desired.

Our cryptosystem changes a plaintext message into a string of numbers. The cipher uses a random assignment of numbers to letters. We used a random number generator to assign the numbers 11 through 36 to the letters A through Z. The assignment is as follows: A=11, B=17, C=14, D=16, E=34, F=24, G=29, H=18, I=19, J=35, K=12, L=28, M=20, N=31, O=33, P=22, Q=30, R=26, S=25, T=27, U=15, V=36, W=32, X=13, Y=21, Z=23. We first multiply each of the above numbers by the randomly chosen encryption key number. This number should be a two digit prime integer. When the multiplication results in a three digit number instead of a four digit number, we add a zero at the beginning. Now, all of our letters are represented by a four digit number. We then substitute the number representation for each letter in our plaintext. We delete any spaces that may be between letters or words and get rid of all punctuation. Thus, we are left with a ciphertext that is a string of numbers.

To decrypt a message, we must know the encryption key, a two digit prime integer. We first separate the string of numbers of the ciphertext into four digit numbers. This can be done by putting a space after each set of four numbers. We then divide each of those numbers by the encryption key, which should always result in a two digit number between 11 and 36. We then substitute the assigned letter (which can be found above) for each two digit number. Then, we use common sense to group the letters into meaningful words and sentences. We now have the plaintext message.

We have created a cryptosystem and cipher that can be used with any randomly chosen encryption key to encrypt text messages sent among employees. This system is small enough that a text message (of up to 140 characters) doesn't result in an encrypted message of more than 5 text messages (or 720 characters); however, it is also secure enough that someone without the encryption key would not be able to decrypt the message and intercept the information. It makes it so that any information leaked on accident will not be understood and taken advantage of by the people who could accidentally receive the text. After the careful and thoughtful work we have invested into this project, we expect that the code will start to pay back through the impossibility of breaking it by anyone who doesn't have the key. This makes us feel secure and satisfied with the work we accomplished. Our code will be easy to implement and will be able to be used to solve the problem of information insecurity of text messages sent within your company.

Sincerely,

[redacted]
Encryption specialists
IMC Inc.