Group K

IMC
Independent Mathematical Contractors, Inc.
136 TMCB
Provo, UT 84602

10 September 2015

OCRA Creative Recursive Acronyms, Inc.
485 Primality Way
Provo, UT 84604

Dear OCRAI:

In response to your request for a nontrivial method of encrypting plaintext English messages we have established a system of encryption which is not only compatible with a standard computer or mobile device keyboard, but benefits from the use.

Our company took a long look at the text messages your members sent to the wrong recipients and devised a system which could have prevented the erroneous breach in security. However, instead of focusing on the messages themselves, our engineers noticed something far more trivial: The time stamp. The time stamp serves as a marker of when the text message was sent, but we created a second way to utilize it: An encryption key.

A time stamp contains three to four numbers indicating the time of the text message's departure as well as an acronym indicating whether the text left "ante meridiem" or "post meridiem." We have utilized these numbers to create a series of one thousand four hundred and forty unique tables which may each individually encrypt the English alphabet and by extension, your company's private conversations.

We do this by constructing the same number of columns in a table as there are hours in the time stamp. The rows begin at the number of minutes and proceed by repeatedly adding the amount contained in the ones place.

For example, if the time stamp read 4:17 AM then four columns would be constructed.

1	2	3	4
…	…	…	…

We would then construct the first row, having it correspond to the number of minutes, in this case, seventeen.

	1	2	3	4
17	…	…	…	…

After which, we begin to add seven to form new rows until we have created enough cells to hold all twenty-six letters of the English alphabet. This pattern would remain the same for any table; for example the rows for 1:03 would increase by increments of three, 2:55 would increase by five, and 7:00 would increase by ten as would any other time stamp ending in zero.

	1	2	3	4
17	**…**	**…**	**…**	**…**
24				
31				
38				
45				
52				
59				

Each of these elements can now hold a number which we create by adding the value of its column and row. For example, the cell at the intersection of column three and row thirty-one would give thirty-four, as we see below.

	1	2	3	4
17	**18**	**19**	**20**	**21**
24	**25**	**26**	**27**	**28**
31	**32**	**33**	**34**	**35**
38	**39**	**40**	**41**	**42**
45	**46**	**47**	**48**	**49**
52	**53**	**54**	**55**	**56**
59	**60**	**61**	**62**	**63**

After this we assign a letter to each number, beginning at A, going left to right and down until we reach Z.

	1	2	3	4
17	**A**	**B**	**C**	**D**
24	**E**	**F**	**G**	**H**
31	**I**	**J**	**K**	**L**
38	**M**	**N**	**O**	**P**
45	**Q**	**R**	**S**	**T**
52	**U**	**V**	**W**	**X**
59	**Y**	**Z**		

However, this is only if the time stamp is ante meridiem. Instead if the time stamp is post meridiem then the last column begins at one and the last row begins with the minute digits. For example 4:17 PM would look like this:

	4	3	2	1
59	**63**	**62**	**61**	**60**
52	**56**	**55**	**54**	**53**
45	**49**	**48**	**47**	**46**
38	**42**	**41**	**40**	**39**
31	**35**	**34**	**33**	**32**
24	**28**	**27**	**26**	**25**
17	**21**	**20**	**19**	**18**

So if Paul Revere were to send Benjamin Franklin a text message at 4:17 AM reading “The Red Coats are coming!” this encryption method would change that to read

“49,28,25,47,25,21,20,41,18,49,48,18,47,25,20,41,39,32,40,27”

With the time stamp of 4:17 AM on his text message, Benjamin Franklin would be able to construct a matrix identical to the one above and therefore be able to decrypt Paul Revere’s message by attaching a preassigned letter to each number. Naturally, the time it takes to construct, encrypt, and send a message would not allow for the above situation to happen simply through human ability. However, a mobile application with the encryption key would easily be able to send, encrypt, and decrypt a text message within a matter of seconds.

Due to the nature of the construction it is almost impossible to decrypt the messages without both the encryption method as well as the key. Furthermore, as there are no punctuation markings besides commas in between letters there would be little way to distinguish one word from another.

Unfortunately in some of the tables duplicate numbers arise as in the matrix we construct for 12:01 AM:

	1	2	3	4	5	6	7	8	9	10	11	12
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
3	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**

	1	2	3	4	5	6	7	8	9	10	11	12
1	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**
2	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**
3	**Y**	**Z**										

It is clear that the above situation would engender difficulty decrypting a message as multiple letters map to one number, such as C, N, and Y all mapping to four. We solved this problem by including first one then two apostrophes as duplicates arise as is clear from the table below:

	1	2	3	4	5	6	7	8	9	10	11	12
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
2	**3’**	**4’**	**5’**	**6’**	**7’**	**8’**	**9’**	**10’**	**11’**	**12’**	**13’**	**14**
3	**4”**	**5”**	**6”**	**7”**	**8”**	**9”**	**10”**	**11”**	**12”**	**13”**	**14’**	**15**

So if the above text message from Paul Revere would have been sent at 12:01 AM instead it would read:

“10’,9,6,8’,6,5,4,5’,2,10’,9’,2,8’,6,4,5’,3’,10,4’,8”

Thus, as you can see, we have developed a complex yet elegant method of substituting numbers for letters using merely the time stamp on your employees’ text messages. Moreover, the largest possible—yet unlikely—output from one hundred forty plaintext characters is six hundred ninety-nine ciphertext characters, less than seven hundred characters and therefore within all of your requirements for the encryption method.

Finally, if we work by Kerckhoff’s principle we may assume that your adversaries will know of this system, but not necessarily the encryption key. Therefore, there will be no mention of the time stamp as the necessary key; instead we will maintain that the key is a random series of three or four numbers necessary to decrypt the text message. Only the creators of the mobile application will need understand the significance of the time stamp to the encryption, anyone else will simply identify it as an ordinary time stamp.

We hope this encryption method meets with your approval and wish to continue to do business with your company in the future.

Sincerely Yours,

[redacted]