[redacted]

Math 485
Project 1

Group L

11 September 2015

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

In today's world, it is simple to send and receive messages and other data. Cell phones, computers with email capability, and tablet devices with an internet connection are ubiquitous. Perhaps because of the easiness of data transfer and the fact that it is now an everyday part of most people's lives, it seems that more and more often sensitive data is made available to people who were not intended to read it. Our client, OCRAI, has been subject to potential leaks of sensitive company data and trade secrets through erroneous text messaging by company employees. We will solve this problem by developing an encryption/decryption process that can be implemented on the phones of all employees of OCRAI, resulting in the secure encryption of all text messages sent and the proper decryption of all messages encrypted by this process.

We begin the encryption of a message with a discussion of which characters are allowed in a plaintext message. In the system we have chosen, the letters of the alphabet (no distinction between uppercase and lowercase), spaces, commas, periods, exclamation points, and question marks may all be encrypted. We will walk through how to use this system by applying the cipher on an example block of plaintext. The plaintext we will use is,

HOW ARE YOU TODAY, FRIEND?

The use of Comic Sans font throughout the rest of this report will indicate either plaintext or ciphertext.

Our first step to encrypt this message is to choose our key. We will use the 6-digit numeric key, (972658). Next we write the integers that correspond to each character in the plaintext in the line above the block to be encrypted.

The integers corresponding to each character are given by the following table.

PT/CT	Int	PT/CT	Int	PT/CT	Int	PT/CT	Int
A	0	I	8	Q	16	Y	24
B	1	J	9	R	17	Z	25
C	2	K	10	S	18	_	26

D	3	L	11	T	19	,	27
E	4	M	12	U	20	.	28
F	5	N	13	V	21	!	29
G	6	O	14	W	22	?	30
H	7	P	15	X	23	Not used	Not used

Thus we would write,

7 14 22 26 0 17 4 26 24 14 20 26 19 14 3 0 24 27 26 5 17 8 4 13 3 30
HOW_ARE_YOU_TODAY,_FRIEND?

Let each number be p_n, where n is the index of characters starting with the first character of the message as 1.
We then process these numbers representing the characters of the message by using the following formula to obtain the encrypted number.

$c_n = 2(k_n) + 3(p_n)(k_{n+1}) \pmod{31}$

Where k_n is the nth digit of the key and $k_1 = k_7 = k_{13} = k_{19}$... etc. In general, $k_{n+6} = k_n$

Thus, $p_1 = 7$ which represents the letter H is changed to

$c_1 = 2*(9) + 3*(7)*(7) \pmod{31}$
$= 165 \pmod{31}$
$= 10 \pmod{31}$

p_2 is changed to

$c_2 = 2*(7) + 3*(14)*(2)$
$= 5 \pmod{31}$

Continuing to change each of the numbers, we end up encrypting our original message as

10-5-28-30-10-10-9-15-2-5-25-5-14-5-27-12-28-1-6-13-0-8-16-0-12-1-17

Writing the message as the characters represented by these numbers we have

kf.?kkjpcfzfof,m.bgnaiqambr

At this point, our encryption is complete. To decrypt this message we simply work in reverse or what we just did to encrypt the message. We would begin by rewriting the encrypted message in a string of integers from 0-30 as in the table above. As we would expect, this results in the string of numbers,

10-5-28-30-10-10-9-15-2-5-25-5-14-5-27-12-28-1-6-13-0-8-16-0-12-1-17

Knowing the formula to change a plaintext character into a ciphertext character is given by

$c_n = 2(k_n) + 3(p_n)(k_{n+1}) \pmod{31}$

We can rewrite this in terms of the plaintext integer, p_n

$$p_n = \frac{1}{3k_{n+1}}(c_n - 2k_n) \ (mod\ 31)$$

This gives us a method of changing the ciphertext integers into the plaintext integers, though it does require us to find the multiplicative inverse of $3k_{n+1}$ for each n. Since we have 31 characters and 31 is a prime number, the gcd($3k_{n+1}$,31) will always be 1, which makes this division possible.

Plugging our first ciphertext integer, $c_1 = 10$, into the given decryption formula, we obtain

$p_1 = (1/21)*(10 - 2*9) \pmod{31}$

To find the multiplicative inverse of 21, we use the extended Euclidean Algorithm[1].

31 = 1(21) + 10
21 = 2(10) + 1

Working backwards, we find

1 = 21 - 2(10)
1 = 21 - 2(31-21)
1 = 3(21) - 2(31) => 3(21) = 1 + 2(31)

Thus the multiplicative inverse of 21 (mod 31) is 3. Using this result, we obtain

$p_1 = 3*(10-18) \pmod{31} = -24 \pmod{31} = 7 \pmod{31}$

[1] See https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm to learn how to use this algorithm

So $p_1 = 7 = H$. For our second ciphertext integer ($c_2 = 5$) we have

$p_2 = (⅙)*(5 - 2*7) \pmod{31} = -5(-9) \pmod{31} = 45 \pmod{31} = 14 \pmod{31}$

So $p_2 = 14 = O$.

Continuing this pattern, we can decrypt the whole message and get back our original plaintext, HOW ARE YOU TODAY, FRIEND?

As we have shown, with our system it is a straightforward matter to encrypt text messages. The implementation of this system on each phone of the employees of OCRAI should be simple. Without the key, recipients of these messages will require significant computing power to break the encryption. Thus unintended recipients of messages containing sensitive company information- who will be without the decryption protocol and key- will not be able to read the messages. Please direct any questions, comments, or concerns to the IMC team found at 136 TMCB, Provo, UT 84602 or through email to [redacted] or [redacted]