Group D [redacted]

OCRA, Inc Technical Report

We received a letter from OCRA, Inc, explaining a problem they had. They have had several text messages containing sensitive and classified information sent to clients and rivals by mistake. OCRA, Inc has asked us to write an encryption method so that the information passed through text can remain classified to those outside of the company. Eventually, a team of engineers will write software to automatically encrypt and decrypt these messages between OCRA, Inc employees. The messages will remain encrypted to anyone outside the company receiving these texts by mistake. We have created an encryption method by which 140 characters will expand to close to 280 characters, and be represented solely by numerals. We want to make sure that our instructions and method cannot be misinterpreted, so as to be clear to the engineers who will eventually write this program. We would be very grateful if you would read this report, and encrypt a message to us using our encryption method. This will help us check our instructions. Thank you for your time and cooperation.

Here are the steps to our encryption method. This method requires an encryption key, consisting of up to ten (10) alpha-numeric characters.

"Stapler" and "2wood"

are examples of two possible encryption keys. This is our first step.

Step two: We begin by creating a 6x6 matrix. The rows and columns are numbered based on the following: We count the number of characters in our encryption key; that number is then the label of the first row and column. We continue labeling the rows and columns in ascending numeric order to 9. Once 9 is reached, if there are remaining rows and columns to label, we continue numbering with 0, 1, 2, etc. For example:

"Stapler" has 7 characters. Thus, our matrix looks like this:

	7	**8**	**9**	**0**	**1**	**2**
7						
8						
9						
0						
1						
2						

"2wood" has 5 characters, so our matrix looks like this:

	5	**6**	**7**	**8**	**9**	**0**
5						
6						
7						
8						
9						
0						

*Note: if we choose an encryption key with 10 characters, we begin labeling rows and columns starting with 0, 1, 2, etc.

Step Three: We then start filling in our matrix. We begin by writing our encryption key, starting in the first row, filling in left to right. We leave out any duplicate letters or numbers that may appear in our key.

For example, our "stapler" matrix begins this way:

	7	**8**	**9**	**0**	**1**	**2**
7	S	T	A	P	L	E
8	R					
9						
0						
1						
2						

And our "2wood" matrix begins like this:

	5	**6**	**7**	**8**	**9**	**0**
5	2	W	O	D		
6						
7						
8						
9						
0						

Step 4: we then completely fill our matrix, starting from a to z, omitting any letters in our encryption key, then we fill in the numerals 0 to 9, also omitting any numerals occurring in our key.

Our complete "stapler" matrix then looks like this:

	7	**8**	**9**	**0**	**1**	**2**
7	S	T	A	P	L	E
8	R	B	C	D	F	G
9	H	I	J	K	M	N
0	O	Q	U	V	W	X
1	Y	Z	0	1	2	3
2	4	5	6	7	8	9

And our complete "2wood" matrix looks like this:

	5	**6**	**7**	**8**	**9**	**0**
5	2	W	O	D	A	B
6	C	E	F	G	H	I
7	J	K	L	M	N	P
8	Q	R	S	T	U	V
9	X	Y	Z	0	1	3
0	4	5	6	7	8	9

Now that our matrix is completed, we can use it both to encrypt and decrypt messages.

Step 5: Encryption. We start with the message we want to encrypt. This message can contain numbers, letters, and spaces. We will call this the "plaintext." We start with the first character of the plaintext, and proceed as follows:

- If the character is a number or letter, we locate it on the matrix.

    - We then replace this character with its location, referred to by first its row number, then its column number. For example, the letter “t” in our “stapler” matrix, is on row 7, and column 8. We will therefore replace “t” with “78” in our ciphertext.
- If the character is a space:
    - We first look at the numbers labeling the rows and columns. We notice that there are 4 numerals from 0 to 9 that we have not used to label the matrix. These numerals are all designated to represent spaces in the plaintext. These are interchangeable, so each time we come to a space, we pick one of these four numerals at random. For example, a space in our plaintext, when encrypting using our “stapler” matrix will be replaced by any of the following: 3, 4, 5, or 6. These are the numerals not used in labeling the rows and columns of the “stapler” matrix.

For example, if our plaintext is, “The duck swims on the lake,” and we are encrypting this message using our “stapler” matrix, the resulting cryptext will be:

78977248009899057701989177407925789772471799072

If we are encrypting the same plaintext on our “2wood” matrix, the resulting cryptext will be:

886966458896576187566078873577928869661775976666

By using this encryption method, we have found a way to represent a common message that looks nothing like the original, and would be quite hard for someone to decrypt without the encryption key. We hope that this method can be efficiently coded to the cell phones of the employees at OCRA, Inc. In this way, their information can remain confidential and within their company. Any outside cell phones receiving an encrypted text will receive nothing but a string of numbers, that they will not be able to easily cipher.