Group A

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

---

8 September 2020

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

Dear OCRAI,

In response to your security requirements, we have developed the [redacted] algorithm—we call it the [redacted] cipher—to automatically encrypt/decrypt messages between authorized personnel. As mentioned in your letter, a common problem in computer security is the human element, which could easily make a mistake or be coerced into leaking sensitive information to malefactors.

Key Security Principles

To ensure security, we decided it was imperative to approach the issue using two security principles—*confusion* and *diffusion*. Confusion is the principle of altering the encoding of a message. This can be seen in substitution ciphers like the Caesar cipher, or in the substitution box phase of AES. The [redacted] algorithm performs confusion by creating a mapping from the original characters to new characters in a way that's dependent on a randomly-generated key, specifically by using the Vigenère cipher (discussed in depth in the Confusion section of this report). Diffusion is the principle of changing one part of the message in a way that changes the entire message as a whole. This can be seen in the use of finite field multiplication in the AES cipher. The [redacted] cipher performs diffusion by organizing the plaintext in row-major order in blocks of square matrices, then after the *confusion* is performed, reading the ciphertext from the blocks in column-major order.

Diffusion Part 1 of 2

We first separate the plaintext into chunks of length 16 and fill a sequence of 4x4 matrices. The matrices are filled in row-major order (left to right, top to bottom). We organize it like so:

1. Take the first 4 characters of the plaintext message and assign them to the first row of the first matrix.
2. Repeat step 1 for each row of the matrix.
3. Repeat steps 1-2 for each successive matrix, until all the plaintext characters are in a matrix.
4. Fill any empty cells in the last matrix with random letters.

We will demonstrate the process with the plaintext "*When it comes to cryptography things get complex quickly*", which has 48 letters. We organize it into three 4x4 matrices, following steps 1-4 above:

W	H	E	N		P	T	O	G		E	T	C	O
I	T	C	O		R	A	P	H		M	P	L	E
M	E	S	T		Y	T	H	I		X	Q	U	I
O	C	R	Y		N	G	S	G		C	K	L	Y

Confusion

The Vigenère cipher is a substitution cipher with a sort of "rolling" key. A key of length n is used to encrypt the message character by character. If the key is shorter than the plaintext, the key is repeated to match the length. Then, the corresponding plaintext and key positions are summed *(mod 26)*. For example, with the plaintext CRYPTO and key BYU, the key is repeated to become BYUBYU, or *[1, 24, 20, 1, 24, 20]* as integers. Then, each character is shifted by its corresponding value in the repeated key: C is increased by 1 to become D, R+24 becomes P, Y+20 becomes S, P+1 becomes Q, T+24 becomes R, and O+20 becomes I. Notice that upon reaching the end of the key, we "roll" to the beginning of the key and continue our substitution process. Hence, encrypting CRYPTO with the key BYU becomes DPSQRI.

Returning to the previous example, we will now use the Vigenère cipher to "confuse" the characters in our matrices. We begin by converting all the letters into integers. "A" is 0, "B" is 1, and as can be figured, "Z" is 25. Here is what our matrices look like now:

22	7	4	13		15	19	14	6		4	19	2	14
8	19	2	14		17	0	15	7		12	15	11	4
12	4	18	19		24	19	7	8		23	16	20	8
14	2	17	24		13	6	18	6		2	10	11	24

Now we apply the Vigenère cipher to these matrices. The key length should be relatively prime to 16 so that the matrices do not start at the same position of the key. Additionally, the key can be randomly generated, so it is not subject to a dictionary attack. To encrypt our message, we will use the key FNVZEJO, which is *[5, 13, 21, 25, 4, 9, 14]* as integers.

The first integer in our key is 5. We will use modular addition to map the first cell of the first matrix to a new cell like so: $23 + 5 = 28 \equiv 2 \pmod{26}$. Using modular addition for the next

6 cells gives 8 + 13 ≡ 21 (mod 26), 5 + 21 ≡ 26 (mod 26), 14 + 25 ≡ 13 (mod 26), 9 + 4 ≡ 13 (mod 26), 20 + 9 ≡ 3 (mod 26), and 3 + 14 ≡ 17 (mod 26), using the next 6 integers from the key. For the next cell (15), we use 5 from the key to get 15 + 5 ≡ 20 (mod 26). Repeating this pattern will result in:

1	20	25	12		10	18	18	15		8	2	16	19
12	2	16	19		5	5	2	2		25	10	10	8
25	25	17	23		23	23	16	22		6	4	25	21
23	16	22	11		18	19	13	5		23	9	15	7

The cells can now be translated back into alphabet characters:

B	U	Z	M		K	S	S	P		I	C	Q	T
M	C	Q	T		F	F	C	C		Z	K	K	I
Z	Z	R	X		X	X	Q	W		G	E	Z	V
X	Q	W	L		S	T	N	F		X	J	P	H

Diffusion Part 2 of 2

We will complete the diffusion of the message by extracting each character from the matrices in column-major order (as opposed to row-major as before), starting with the first matrix. We begin by removing the first column [B, M, Z, X] and writing it onto a horizontal line. Repeat this for every column. The resultant ciphertext is:

BMZXUCZQZQRWMTXLKFXSSFXTSCQNPCWFIZGXCKEJQKZPTIVH

Decryption

To decrypt, perform the encryption steps in reverse:

1. Organize the ciphertext into 4x4 matrices in column-major order, by matrix.
2. Translate the letters into their 0-indexed numerical representations.
3. Perform modular subtraction using the Vigenère cipher key. For example, the first cell in the first matrix has a 2. Subtract it by the first integer of the key. This results in 2 - 5 = -3 ≡ 23 (mod 26).
4. Translate the numbers into their alphabetic representations.
5. Write each character out in row-major order, by matrix.

This results in the plaintext:

WHENITCOMESTOCRYPTOGRAPHYTHINGSGETCOMPLEXQUICKLY

Insert the spaces in between distinguishable words and the ciphertext is completely decrypted:

When it comes to cryptography things get complex quickly

If a word at the end of the plaintext does not resemble a dictionary word, assume it was random letter padding and discard it.

In Summary

As explained above, the [redacted] cipher applies the principle of confusion in tandem with diffusion to protect sensitive information from prying actors. Our algorithm is more secure than a simple substitution cipher because the use of diffusion makes it difficult to discern the order of the Vigenère cipher, and the use of the Vigenère cipher causes greater difficulty to attacks trying to decrypt the message. Letter frequency count is weakened because the attacker must be able to accurately group which letters correspond to which position of the encryption key, and even then the frequency is 1/n the size of the message body, leading to a much smaller sampling size for analysis.

We have determined that through application of the [redacted] cipher, the messages sent between employees will be much more secure, and should a recipient error occur again the message shouldn't be immediately discernible. However, our full recommendation would be to restrict messaging between authorized persons participating in the app, such that messages could never leak to an outside actor and thus expose company information to those who would exploit it. We also posit that our encryption could be strengthened by including a transposition within the grid to further diffuse the cipher text and increase the encryption strength, per Kerckhoff's principle of relying upon key secrecy rather than algorithm secrecy.

Yours securely,

[redacted]

Founders
Independent Mathematical Contractors, Inc.