Group F

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,

Privacy when sending messages is very essential in any business. We are glad you came to us to help in your time of need. We propose a simple Electronic Codebook (ECB) solution to your encryption problem. It is a simple system that can work for text messages and can be extended to handle your future needs.

The encryption method is simple. Each character is encoded in ASCII and can be represented as two hexadecimal digits or eight binary digits (bits). A conversion table for many of the commonly used characters is listed below.

Char	Hex	Bin	Char	Hex	Bin	Char	Hex	Bin	Char	Hex	Bin
<space>	20	0010 0000	5	35	0011 0101	M	4D	0100 1101	f	66	0110 0110
!	21	0010 0001	6	36	0011 0110	N	4E	0100 1110	g	67	0110 0111
“	22	0010 0010	7	37	0011 0111	O	4F	0100 1111	h	68	0110 1000
#	23	0010 0011	8	38	0011 1000	P	50	0101 0000	i	69	0110 1001
$	24	0010 0100	9	39	0011 1001	Q	51	0101 0001	j	6A	0110 1010
%	25	0010 0101	:	3A	0011 1010	R	52	0101 0010	k	6B	0110 1011
&	26	0010 0110	;	3B	0011 1011	S	53	0101 0011	l	6C	0110 1100
‘	27	0010 0111	?	3F	0011 1111	T	54	0101 0100	m	6D	0110 1101
(	28	0010 1000	@	40	0100 0000	U	55	0101 0101	n	6E	0110 1110
)	29	0010 1001	A	41	0100 0001	V	56	0101 0110	o	6F	0110 1111
*	2A	0010 1010	B	42	0100 0010	W	57	0101 0111	p	70	0111 0000
+	2B	0010 1011	C	43	0100 0011	X	58	0101 1000	q	71	0111 0001
,	2C	0010 1100	D	44	0100 0100	Y	59	0101 1001	r	72	0111 0010
-	2D	0010 1101	E	45	0100 0101	Z	5A	0101 1010	s	73	0111 0011
.	2E	0010 1110	F	46	0100 0110	\	5C	0101 1100	t	74	0111 0100

/	2F	0010 1111	G	47	0100 0111	_	5F	0101 1111	u	75	0111 0101
0	30	0011 0000	H	48	0100 1000	a	61	0110 0001	v	76	0111 0110
1	31	0011 0001	I	49	0100 1001	b	62	0110 0010	w	77	0111 0111
2	32	0011 0010	J	4A	0100 1010	c	63	0110 0011	x	78	0111 1000
3	33	0011 0011	K	4B	0100 1011	d	64	0110 0100	y	79	0111 1001
4	34	0011 0100	L	4C	0100 1100	e	65	0110 0101	z	7A	0111 1010

For example, the word “Text” would be written as seen below:
5 4 6 5 7 8 7 4 Which could then be converted to the following:
0101 0100 0110 0101 0111 1000 0111 0100 This is the code of the plaintext.

To encrypt the plaintext, we need a key which consists of four hexadecimal digits (labeled Hex in the chart). A table listing the hexadecimal digits with their binary representations is listed below. In our example, we use 74AF as our key.

Hex	Bin		Hex	Bin		Hex	Bin		Hex	Bin
0	0000		1	0001		2	0010		3	0011
4	0101		5	0101		6	0100		7	0111
8	1000		9	1001		A	1010		B	1011
C	1100		D	1101		E	1110		F	1111

We write the key in terms of bits.
7 4 A F
0111 0100 1010 1111

We write the key under the plaintext and keep repeating the key until we reach the end of the text.
0101 0100 0110 0101 0111 1000 0111 0100 plain text written as bits
0111 0100 1010 1111 0111 0100 1010 1111 The key repeated

Now we perform a bitwise exclusive-or or add each column using modulo 2. (In other words, 0+0=2, 1+1=0, 0+1=1+0=1)

0101 0100 0110 0101 0111 1000 0111 0100 plain text written as bits
<u>0111 0100 1010 1111 0111 0100 1010 1111</u> The key
0010 0000 1100 1010 0000 1100 1101 1011 This is now the ciphertext.

To decrypt the message, we will write the key beneath and add the digits mod2 again.

0010 0000 1100 1010 0000 1100 1101 1011	The ciphertext.
0111 0100 1010 1111 0111 0100 1010 1111	The key
0101 0100 0110 0101 0111 1011 0111 0100	This is the original plain text written as bits.

Using our key in table 1, we can convert the bits back into hexadecimal
54 65 78 74 and then convert those into characters and we get
T e x t.

So, even if the encryption method is known, your message will remain secure as long as no one knows they key. In addition, our encryption method can be strengthened by increasing the key size. It can also be extended to provide encryption for any electronic communication. Finally, with a little added complexity, we can convert our encryption algorithm to Cipher Block Chaining (CBC) to allow even more secure encryption for audio and image messages. We hope you return to us for your future encryption needs.

Sincerely,

Independent Mathematical Contractors, Inc.