Data Encryption Using Multi Codes For One Character (MCFOC)

Firas Layth Khaleel Alameen
University Utara Malaysia: Malaysia \ Kedah \ Changlon \ Sintok \UUM\CAS college
Tikrit University: Iraq \ Salah Din \ Tikrit \ Alqadisiya \ TU \ college of Computer Science and Math
Firas_Layth@yahoo.com

Abstract

We offer a way to encrypt messages sent over the network. The objective of this project is to hide information in the message .The format is innovative, modern and durability depends on the strength of the algorithm used since this method is difficult to decipher hacker easily, because the field of encryption in this way is very wide and several cryptographic options.

.

Key Words: Data Encryption, multi codes, (MCFOC), Cryptography

1. Introduction

Cryptography is one way of providing security using the process of encryption and decryption. In general any encryption and decryption scheme uses symmetric key algorithms like DES, RC5, IDEA etc...
Cryptography has long been in use by governments, particularly in the realms of military and diplomatic communication. It is hard to imagine military communication without cryptography; cryptanalysis, or secretly deciphering the opponent's messages, is perhaps of even greater value. Much has been written about cryptography in the military; see reference [l] for example. During the early 1970s, it became apparent that the commercial sector also has a legitimate need for cryptography. Corporate secrets must be transmitted between distant sites, without the possibility of eavesdropping by industrial spies. Personal data on databases need to be protected against espionage and alteration. A familiar example is the communication between an automatic teller machine (ATM) and a central computer. The user inserts a magnetic card and types a few numbers. The ATM sends messages to the computer. The computer checks the account balance and returns a message authorizing the ATM to dispense funds. Obviously, if these messages are unprotected, a thief can tap the wires, find the message authorizing the dispensing of funds, and send multiple copies of that message to the ATM, thereby "cleaning out'' the supply of cash from the ATM. develop a system for encrypting ATM data.
This paper has four sections. After this introduction, Section 2 Certification technical new ideas. After that System Implementation is presented in Section 3. Finally Section 4 contains the conclusion and the scope for future research.

2. Certification technical new ideas

- **Purpose :** The purpose of this software is to encrypt the message sent using a very sophisticated way to encrypt the data so as to ensure no leakage of sensitive and confidential information when do a sending

- **Design/methodology/approach :** Design a software that converts each character in a message to 4 (decimal numbers or hexadecimal number) but each character has minimum 4 codes...

- **Findings /or expected findings :** For the expected results are difficult to decipher the message because we will use multi code for one character in one time when the character passing through the message.
  Like 'A' = **4499,9876,1267,6291**

- **Research limitations/implications :** The main objective of the software is to maintain the security of information transmitted via modern means of transportation such as the Internet and mobile, and so on....

- **Practical implications :** This research focused on making the encryption process is not complex and simple at the same time there can not be solved easily. If Allah willing in this research , they can develop all the software for encryption and security of information, especially in countries where governments are electronic.....

- **Originality/value :** This Demo has been programmed in a language Java and is the first step for us…

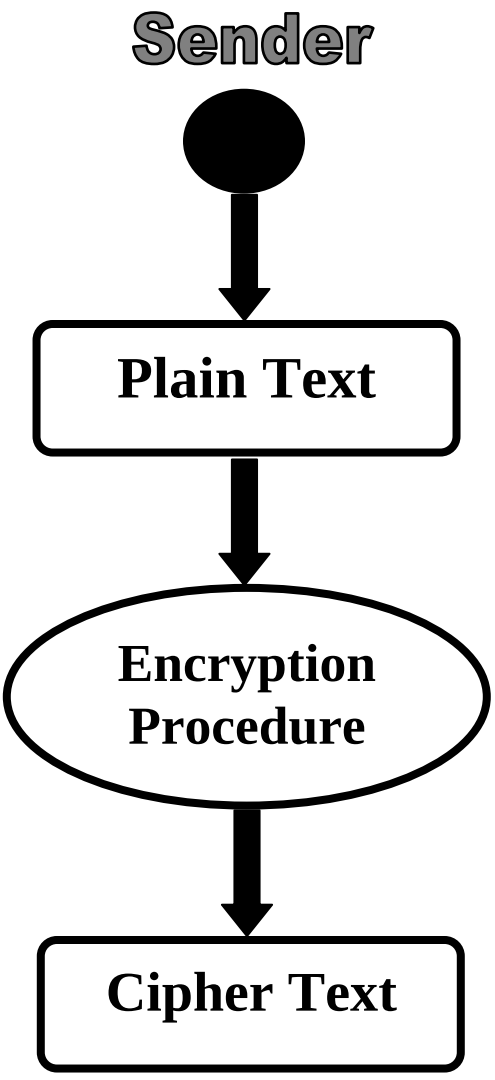

Figure (1 - A)

This Figure (1 - A) (**Sender**) Who responsible for converting plain text into cipher text, .

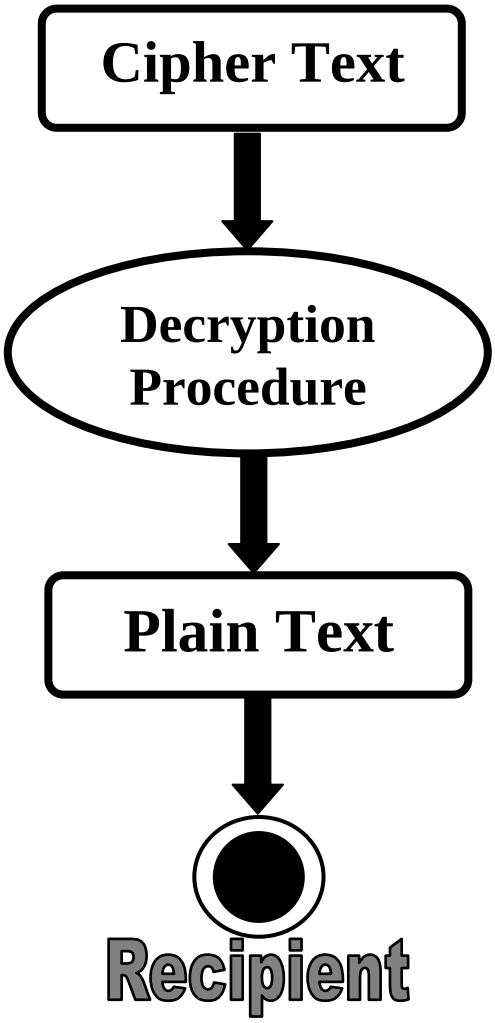

Figure (1 - B)

This Figure (1 - B) (**Recipient**) Who responsible for converting the cipher text to the a plain text .

3. System Implementation

This system works to convert plain text to encrypted text by using the special procedures .
Where these procedures are working to convert each code in the letter from , plain text to to (decimal numbers or hexadecimal number) . Programmed according to the work and every one of the numbers are made up of at least 4 codes and each code has at least 4 numbers For example 'A' has 4 codes = (**4499,9876,1267,6291**) .

Where when you see the character A in the simple text capital , it will change to the first code of **4499** and when see in plain text again, and its capital , it will change to **9876** and the third time be a code of 5464 and the fourth be code is **1267** .And when it appears for the fifth time the same code of the first code is **6291** and so on .
Loop , we will be use to change the character codes at least 4 times, and then repeated back to the first code .
we will show you a better way, so that the process will be a table that contains all the characters required to write in plain text and we will show a simple example for how the characters changes from plain text to cipher text .

No	Character	Multi codes Example Decimal number From 0000 to 9999
1	**A**	**4499,9876,1267,6291**
2	**B**	**3333,9865,9128,6239**
3	**C**	**3311,9854,7346,9371**
4	**D**	**3322,9843,6519,9218**
5	**E**	**3344,9832,8118,9477**
6	**F**	**4455,9821,7117,7821**
7	**G**	**5566,9810,6116,8810**
8	**H**	**3377,9899,5115,4501**
9	**I**	**3388,9878,9338,2037**
10	**J**	**3399,9867,5116,7056**
11	**K**	**2222,9856,5638,5693**
12	**L**	**2211,9845,5636,5637**
13	**M**	**2233,9834,8016,8017**
14	**N**	**2244,98238014,8015**
15	**O**	**2255,9812,8012,8013**
16	**P**	**2266,9801,8010,8011**
17	**Q**	**2277,8007,8008,8009**
18	**R**	**2288,8004,8005,8006**
19	**S**	**2299,8001,8002,8003**
20	**T**	**2200,7007,7008,7009**
21	**U**	**1100,7004,7005,7006**
22	**V**	**2200,7001,7002,7003**
23	**W**	**3300,6007,6008,6009**
24	**X**	**4400,6004,6005,6006**
25	**Y**	**5500,6001,6002,6003**
26	**Z**	**6600,5008,5009,5007**
27	**a**	**7700,5005,5002,5004**
28	**b**	**8800,4001,4002,4003**
29	**c**	**9900,3001,3002,3003**
30	**d**	**0011,2563,2580,2509**
31	**e**	**0022,2467,2478,2489**
32	**f**	**0033,4349,4398,4309**
33	**g**	**0099,4346,4347,4348**
34	**h**	**0066,2567,2500,2590**
35	**i**	**0088,2389,2321,2356**
36	**j**	**0055,1895,1896,1799**
37	**k**	**0077,0097,0096,0094**
38	**l**	**0044,0091,0097,0095**
39	**m**	**9988,6650,6640,6680**
40	**n**	**9977,6690,6610,6670**
41	**o**	**9966,6756,6620,6630**
42	**p**	**9955,6723,6734,6745**
43	**q**	**9944,6767,6798,6712**
44	**r**	**9933,7251,6745,6746**
45	**s**	**9922,7512,7519,7510**
46	**t**	**9911,7412,7413,7411**
47	**u**	**8899,7416,7417,7414**
48	**v**	**8888,7510,7911,7912**
49	**w**	**8877,7956,7057,7958**
50	**x**	**8866,8237,8238,8219**
51	**y**	**8855,8231,8235,8236**
52	**z**	**8844,7295,7293,7294**
53	**0**	**8833,7629,7630,7631**
54	**1**	**8822,4820,4821,4823**
55	**2**	**8811,1234,5678,9101**
56	**3**	**7777,1213,1415,1617**
57	**4**	**7799,1819,2021,2223**
58	**5**	**7788,3456,6789,7357**
59	**6**	**7766,0228,0619,0741**
60	**7**	**7755,0906,0973,0268**
61	**8**	**7744,1808,1909,1000**
62	**9**	**7733,1505,1606,1707**
63	**+**	**7722,1202,1303,1404**
64	**-**	**7711,1289,1267,1245**
65	**/**	**6655,1290,1380,1470**
66	*****	**6699,1140,1130,1120**
67	**&**	**6688,1160,1160,1150**
68	**^**	**6677,1109,1180,1170**
69	**%**	**6666,1193,1192,1190**
70	**$**	**6644,1196,1195,1194**
71	**#**	**6633,1191,1198,1197**
72	**@**	**6622,1156,1167,1178**
73	**!**	**6611,1132,1134,1145**
74	**(**	**0000,5959,5105,1121**
75	**)**	**5555,5656,5757,5858**
76	**{**	**5599,5151,5252,5353**
78	**}**	**5588,5433,5454,5145**
79	**[**	**5577,5122,5211,5311**

80	]	**5566,5677,5788,5899**
81	'	**5544,5667,5778,5889**
82	"	**5533,7112,5223,5334**
83	;	**5522,5691,5663,5667**
84	:	**5511,6795,6796,6969**
85	.	**5500,7894,7895,7896**
86	,	**4444,7867,7892,7893**
87	<	**4411,7834,7845,7856**
88	>	**4422,7566,7813,7812**
89	?	**4433,7909,7989,7519**
90	\	**4455,8222,8765,8861**
91	|	**4488,8045,8056,8067**
92	`	**4466,8766,8012,8023**
93	~	**4477,9005,9006,9006**

Table (1)

This table has 93 characters and each one has 4 codes and each code has 4 numbers .

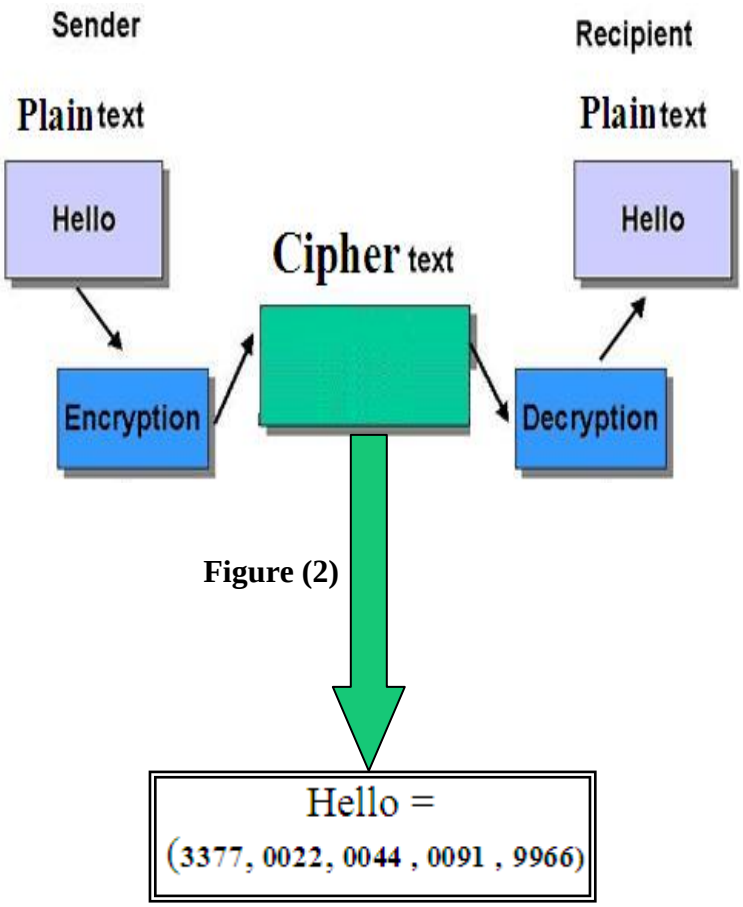

Figure (2)

We will show another example to explain how to engine the operation for the multi coding in this table

No	Character	Multi codes Example Decimal number
1	**A**	**4499**
2	**AA**	**4499, 9876**
3	**AaAa**	**4499, 7700, 9876,5005**
4	**BBbb**	**3333,9865, 8800,4001**

Table (2)

4. Conclusions

In these papers show the following:

- Difficult to decode cipher text so as to contain more than one code for the character and also contain more than one number for the code we have used, for example consisting of 4 digits.
- As well as for the characters we used the formula for capital letter and small letter .
- The strength of this procedure depend on the number of codes for each character and the number of digits of each code any direct proportion to the strength of encryption used.
- Results obtained in this analysis indicates that the encryption and decryption are completely in agreement with each other.

5- References

[1] B.R. MSVS, V Vardhan B, Naidu G A, P.Reddy L, V Babu A "*A Noval Security Model for Indic Scripts*", International Journal of Computer Science and Security, (IJCSS) Volume (3) : Issue (4) , PP 303 – 313 .

[2] S.U Kumar, V.U.K. Sastry, A.V Babu,." *A Block Cipher Basing Upon a Revisit to the Feistel Approach and the Modular Arithmetic Inverse of a Key Matrix* ", IAENG International Journal of Computer Science, 32:4, IJCS_32_4_1. (Advance online publication: 12 November 2006).

[3] D. Coppersmith , "*The Data Encryption Standard (DES) and its strength against attacks*" IBM J. RES. DEVELOP. VOL. 38 NO. 3 MAY 1994, PP 243-250

[4] FangYing-lan Han Bing Li Ye-bai,*" Exploration and Research based on VIN Code Vehicle Identification System"* 2009 International Conference on Industrial and Information Systems , Authorized licensed use limited to: UNIVERSITI UTARA MALAYSIA. Downloaded on August 10,2010 at 16:49:53 UTC from IEEE Xplore. Restrictions apply, PP 324 – 326 .

[5] Moceheb Lazam Shuwandy, Ali Khalil Salih, Firas Layth Khaleel Alameen, and Adib M.Monzer Habbal. IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, 2010. 136-140.

Eng. Firas Layth Khaleel Alameen. I'm graduated from AL-RAFIDAIN University College in Baghdad , Department of Software Engineering (2003-2004) and I have B.S.c In Software Engineering. I have been appointed at Tikrit University after having a B.S.c degree , as a programmer in internet and computer unit . After six month of my appointment date I have been appointed as a manager of internet and computer unit .Now I'm student M.S.c (IT) in University of Utara in Malaysia(UUM) This is 1st semester of Information Technology (2009-2010).