Encryption of Data into a New Pattern Which Depends on Password Content Set by User

Uday Bhaskar

ABSTRACT: Encryption of data is important to maintain privacy and secure important data. We generally use a password to protect our important and confidential files but think of a encryption which depends on password content set by user to encrypt the contents of the file into a highly secure encryption. In this proposed method of encryption the data is first converted into a newly designed 4 bit format, further it is then changed to a Gray code format of 4 bits and finally every 2 bits is paired as one, this makes every letter equivalent to 8 bit. This encryption provides a better way to secure data using new format of coding.

INDEX TERMS - Encryption, Gray Code, ASCII, Bits, Privacy, Security

---

1. INTRODUCTION

To ensure privacy and security the data must be encrypted in a format that is none discoverable by outside programs or people. The encryption includes conversion from one format to other. This includes conversion to a new proposed format, ASCII codes and gray codes. The encryption and decryption of data is easy if one knows the method along-with the password. The password defines the way in which the data is to encrypted. From the contents of password only the encryption type is to be encrypted.

2. BACKGROUND

As being a Computer Science and Engineering Student I became familiar with the field of encryption and Cryptography. As all of us have used password protected system to secure our private and confidential data. I always thought of designing our own Secure and encrypted system.

- *UDAY BHASKAR is currently pursuing bachelor degree program in Computer Science and engineering in VIT University, Vellore, INDIA, PH-+919677476970. E-mail: udaybhaskar455@gmail.com*

3. PROPOSED METHODOLOGY

Here is the new proposed method of encryption, the whole method is proposed in 4 steps stated below.

A. Step 1 :- A new format is proposed based on the no. of bits to be included i.e. M and the real number which is to be used for defining the format denoted by N and K= length of password.

M – 2,3,4 and so on. N - 2,3,4,5,6… so on

The value of N and M depends on the password content set by user, if password length is 8 characters then M=2, N=6, we calculate M=3 & N=6 for K=9 using formula stated below.

$$N = K/3 \quad \& \quad M = K-N$$

Password length is Restricted between 8 characters to 16 characters and for K=8 we have N=M=4 as predefined.

Example:- Let the sentence be "DEFINE"

Each letter in the Sentence above has its own ASCII code and they are

ASCII CODE:- 68 69 70 73 78 69

If we take M=3 and N=4 , then the above code is converted to

68 = "2112", 69 = "2120", 70 = "2121", 78= "2220"

So, DEFINE = 2112-2120-2120-2121-2220

For M=4 and N=4, we have

DEFINE = 1010-1011-1012-1021-1032-1011

The format for Values of M = 4 and N = 3, 4 and N= 5 & M=3 respectively as follows.

TABLE 1(M=4 & N=3)

	M_4	M_3	M_2	M_1
	(27)	(9)	(3)	(1)
0	0	0	0	0
1	0	0	0	1
2	0	0	0	2
3	0	0	1	0
4	0	0	1	1
5	0	0	1	2
6	0	0	2	0
7	0	0	2	1
8	0	0	2	2
9	0	1	0	0
10	0	1	0	1
11	0	1	0	2
12	0	1	1	0
.				
.				
.				
80	2	2	2	2

TABLE 2(M=4 & N=4)

	M_4	M_3	M_2	M_1
	64	16	4	1
0	0	0	0	0
1	0	0	0	1
2	0	0	0	2
3	0	0	0	3
4	0	0	1	0
5	0	0	1	1
6	0	0	1	2
7	0	0	1	3
8	0	0	2	0
9	0	0	2	1
10	0	0	2	2
11	0	0	2	3
12	0	0	3	0
.				
.				
.				
215	3	3	3	3

TABLE 3(M=3 & N=5)

	M_3	M_2	M_1
	25	5	1
0	0	0	0
1	0	0	1
2	0	0	2
3	0	0	3
4	0	0	4
5	0	1	0
6	0	1	1
7	0	1	2
8	0	1	3
9	0	1	4
10	0	2	0
11	0	2	1
12	0	2	2
.			
.			
.			
124	4	4	4

M has four bits namely M_1, M_2, M_3, M_4 .

To calculate the value of Decimal from given values of N, M_1, M_2, M_3, M_4 one need to calculate using the formula

$$Decimal\ VALUE = (M_1 * N^0) + (M_2 * N^1) + (M_3 * N^2) + (M_4 * N^3)$$

The formula to calculate the total no. of decimal values for specified values of N and M is $[M^{N-1}]$

B. ***Step 2 :-*** Once we get the encrypted code from the first step then every bit is further converted to the gray code .Gray code is a 4-bit code which can be converted to Binary Coded Decimal and Decimal format using the Table 4 given below. For example, the code obtained from above step is as follows:-

TABLE 4

Conversion Table of BCD & Gray Code

DECIMAL	GRAY	BCD
0	0000	0000
1	0001	0001
2	0011	0010
3	0010	0011
4	0110	0100
5	0111	0101
6	0101	0110
7	0100	0111
8	1100	1000
9	1101	1001
10	1111	1010

11	1110	1011
12	1010	1100
13	1011	1101
14	1001	1110
15	1000	1111

Now we proceed by converting to gray code after obtaining result from step 1.

From Step1, DEFINE = "1010-1011-1012-1021-1032-1011" for M=4 and N=4.

On converting to gray code, the following code is obtained:-

DEFINE:-"0001000000010000-0001000000100010001-0001000000010011-0001000000010011-0001000000100011-0001000000010001"

C. STEP 3 :- Finally every two bit is converted to 0,1,2,3 depending on input. If we take 00 it is converted to 0 using TABLE 5. This will make the encryption more precise and reduce the 16 bit format to 8 bit format and the final code obtained will consist of only four bits 0,1,2,3 .

TABLE 5

INPUT	OUTPUT
00	0
01	1
10	2
11	3

Now we convert the above result obtained from Step2 by selecting 2bit in pair using the above table

DEFINE=
"01000100010001010100010301000103010002030100010 1"

D. *STEP 4 :-* The below code obtained is the final encrypted code for the word "DEFINE"

DEFINE=
"01000100010001010100010301000103010002030100010 1"

To decrypt the code just follow the reverse order for the steps involved in encryption:-

Step1 :- Each bit is to converted to 2 bit using table 5 .

*Step2 :-*Then convert the gray code obtained from step1 to BCD using table 4.

Step3:- Then convert to ASCII code by taking group of 4 Bit.

Step4:- From ASCII code obtained in Step3 convert to original data.

4. CONCLUSION

The main motive of this method is to provide secure encrypted code for the files and data in it. It will help to secure confidential and private data. I proposed this idea to give a new way of encryption. This encryption code is more reliable and efficient.

5. ACKNOWLEDGEMENT

I would like to thank everybody who supported me in completing this project, the authors for their references and specially God for providing an opportunity to do so. Special thank to my teachers, Parents and friends.

6. REFERENCES

[1] http://en.wikipedia.org/wiki/Encryption

[2] http://en.wikipedia.org/wiki/Ascii

[3] http://en.wikipedia.org/wiki/Gray_code

[4] http://en.wikipedia.org/wiki/Cryptography