Prestige e-Journal of Management and Research
Volume 3, Issue 1(April 2016)
ISSN 2350-1316

DUAL SECURED DATA TRANSMISSION USING ARMSTRONG NUMBER AND COLOR CODING

Vaibhav Kant Singh*

With the advent and evolution of Computing and Internet technology, there is a drastic change in the general manner communication between individuals. Today people use technology for doing almost all basic things. All individuals with the wide usage of mobile phones (Specifically Smart Phones) are able to communicate with each other. Smart phones enable user to use internet facility very easily, also with the facility of hotspot connection which could be made with laptop, the usage is easy and useful. Internet gave platform for the user to do a variety of actions like shopping, getting information about various aspects, booking tickets, chatting etc. While doing all these actions using internet, various personal information of the sender is exposed to the intruders sitting in the internetwork. These intruders use the private pieces of information like internet banking password of Individuals (which might be exposed during internet shopping) for taking advantage. There are several approaches which are currently running to have protection against these intruders. New mechanisms for making the internet communication secure are always a potential area for research. In this paper the author proposed a dual secured data transmission mechanism for protecting the data from being identified by the intruder. In the proposed method, at first level a color code is used by the sender for authentication and in the second level Armstrong number is used for encryption. Armstrong number used for encryption is a nice technique for providing security. How encryption using Armstrong number is going to take place is discussed in the paper by the author. The data received at the receiver end whether by the intruder or by the authorized receiver, could be retrieved only if the receiver is able to enter the password to the application which the sender has set. The password is a combination of color, set from the color palette available in the communication application. The cracking of the color code set as password for reading data is a tough task. Application for performing the task is implemented and discussed in the paper.

Keywords: Armstrong Number, Intruder, Security, Encryption, Decryption.

---

*Department of Computer Science and Engineering, Institute of Technology, Guru Ghasidas Vishwavidyalaya, Central University Bilaspur, Chhattisgarh, India,

INTRODUCTION

With the advent of computing technology the processing of data and data communication has reached a great level. The cost of hardware in terms of capability to perform tasks is decreasing day by day. This has aroused a situation where more and more people are involved in adopting computing technology as a medium to deliver their useful data processing task. In computing technology, software development is a very major field. To meet the competitive demands of the users the software developers are engaged in making good quality software that can satisfy the user. The Software that is delivered to the customer should satisfy some set of quality measures like:-

1. Integrity
2. Correctness
3. Portability
4. Openness and Interoperability
5. Security
6. Maintainability
7. Reusability etc.

Software which is going to be delivered to the customer is going to be checked for the above evaluation measures. In the paper, the author is making a focus on security a very important aspect in the current scenario.

Problem Statement

The software that is delivered to the customer must meet the security constraint. Thus providing security to the software from unauthorized access is the motive of the work. In this paper we will lay focus on the way that could be adopted by the developer to ensure security in the internet for the application developed by them.

REVIEW OF LITERATURE

Singh et al. (2015) had discussed fraud detection in cloud framework. Singh et al. (2010) had proposed data-mining a step in the KDD process as an efficient technique for detecting fraud in the digital data on the basis of the survey made on the subject. Singh and Singh (2010) proposed a dual digital marking system for providing security in data transmission. Singh and Singh (2015a) proposed color coding mechanism for providing security over the Internet. Singh and Singh (2015b) proposed dual level digital signature for providing security.

Proposed Work

The method proposed is going to provide two level security to the transmitted data. In the first level we will implement the use of color code for authentication purpose. If the person in the destination machine is having the information of the color code set as password then only he will be able to open the documentation. Beside to the first level security implemented by means of authentication the second level security may be implemented by means of encryption through ARMSTRONG color coding technique.

Encryption Process [Source Machine]
PHASE-1

The person who is sending message is going to set a password i.e. color oriented a combination of red, green and blue. The values of each are going to range in between 0-255. A number of color combinations could be made of this. Only the Person who is sending and who is going to receive the message is going to have knowledge about the combination. Thus, it is hard to crack.

PHASE-2
Suppose the message to be encrypted is "VAIBHAV SINGH"

The procedure to be adopted is as follows:-

Step1:-MESSAGE:"V A I B H A V S I N G H" **ARMSTRONG number:** 371

Message	V	A	I	B	H	A	V	S	I	N	G	H
ASCII Code (x)	86	65	73	66	72	65	86	83	73	78	71	72
Armstrong Number (y)	3	7	1	9	49	1	27	343	1	3	7	1

First Step Encrypted Message W =(x+ y)	89	72	74	75	121	66	113	426	74	81	78	73

Step2:-The encrypted message is put into 3x4 matrix named "A" as represented below:-

$$A = \begin{bmatrix} 89 & 75 & 113 & 81 \\ 72 & 121 & 426 & 78 \\ 74 & 66 & 74 & 73 \end{bmatrix}$$

Step3:- ARMSTRONG number taken represented in form of MATRIX "B" of 3x3 form

$$B = \begin{bmatrix} 3 & 7 & 1 \\ 9 & 49 & 1 \\ 27 & 343 & 1 \end{bmatrix}$$

Step4:- Cipher text produced in the source machine to be sent to the destination machine is represented by Matrix "C" $Cipher\ Text\ (C) = B \times A$

$$C = \begin{bmatrix} 845 & 1138 & 3395 & 862 \\ 4403 & 6670 & 21965 & 4624 \\ 27173 & 43594 & 149243 & 29014 \end{bmatrix}$$

Step5:- Final Encrypted Message is:

$$[845 \quad 4403 \quad 27173 \quad 1138 \quad 6670 \quad 43594 \quad 3395 \quad 21965 \quad 149243 \quad 862 \quad 4624 \quad 29014]$$

Decryption Process [Destination Machine]:

Phase1:

Phase2:

Step1: Generate of Matrix "D" as Follows

$$D = B^{-1}$$

Since,

$$B^{-1} = \frac{Adj\ of\ (B)}{|B|}$$

$$Adj\ of\ (B) = [Cofactor\ of\ (B)]^T$$

$$Cofactor\ of\ (B) = \begin{bmatrix} +\begin{vmatrix} 49 & 1 \\ 343 & 1 \end{vmatrix} & -\begin{vmatrix} 9 & 1 \\ 27 & 1 \end{vmatrix} & +\begin{vmatrix} 9 & 49 \\ 27 & 343 \end{vmatrix} \\ -\begin{vmatrix} 7 & 1 \\ 343 & 1 \end{vmatrix} & +\begin{vmatrix} 3 & 1 \\ 27 & 1 \end{vmatrix} & -\begin{vmatrix} 3 & 7 \\ 27 & 343 \end{vmatrix} \\ +\begin{vmatrix} 7 & 1 \\ 49 & 1 \end{vmatrix} & -\begin{vmatrix} 3 & 1 \\ 9 & 1 \end{vmatrix} & +\begin{vmatrix} 3 & 7 \\ 9 & 49 \end{vmatrix} \end{bmatrix}$$

$$Cofactor\ of\ (B) = \begin{bmatrix} -294 & +18 & +1764 \\ +336 & -24 & -840 \\ -42 & +6 & +84 \end{bmatrix}$$

$$[Cofactor\ of\ (B)]^T = \begin{bmatrix} -294 & 336 & -42 \\ +18 & -24 & +6 \\ 1764 & -840 & +84 \end{bmatrix}$$

$$Adj\ of\ (B) = [Cofactor\ of\ (B)]^T$$

$$B^{-1} = \frac{Adj\ of\ (B)}{|B|}$$

Now Since,

$$B = \begin{bmatrix} 3 & 7 & 1 \\ 9 & 49 & 1 \\ 27 & 343 & 1 \end{bmatrix}$$

Therefore,

$$|B| = 1008$$

Putting the value of $|B|$ and $Adj\ of\ (B)$in the Equation for B^{-1}we get

$$B^{-1} = \frac{1}{1008}\begin{bmatrix} -294 & 336 & -42 \\ +18 & -24 & +6 \\ 1764 & -840 & +84 \end{bmatrix}$$

Therefore Matrix D is a Follows

$$D = B^{-1} = \begin{bmatrix} \frac{-7}{24} & \frac{1}{3} & \frac{-1}{24} \\ \frac{1}{56} & \frac{-1}{42} & \frac{1}{168} \\ \frac{7}{4} & \frac{-5}{6} & \frac{1}{12} \end{bmatrix}$$

Step2:- Decrypted message will evaluated for the Matrix D as Follows:

$$Decrypted\ Message = D \times C$$

$$\boldsymbol{D \times C} = \begin{bmatrix} \frac{-7}{24} & \frac{1}{3} & \frac{-1}{24} \\ \frac{1}{56} & \frac{-1}{42} & \frac{1}{168} \\ \frac{7}{4} & \frac{-5}{6} & \frac{1}{12} \end{bmatrix} \times \begin{bmatrix} 845 & 1138 & 3395 & 862 \\ 4403 & 6670 & 21965 & 4624 \\ 27173 & 43594 & 149243 & 29014 \end{bmatrix}$$

$$Decrypted\ Matrix\ X^C = \begin{bmatrix} 89 & 75 & 113 & 81 \\ 72 & 121 & 426 & 78 \\ 74 & 66 & 74 & 73 \end{bmatrix}$$

Step3: Converting the value of Matrix X^C in decrypted message

Decrypted Code from Matrix X^C	89	72	74	75`	121	66	113	426	74	81	78	73
Armstrong Number (y)	3	7	1	9	49	1	27	343	1	3	7	1
Decrypted Original Message W=(x^c-y)	86	65	73	66	72	65	86	83	73	78	71	72
Equivalent ASCII Code	V	A	I	B	H	A	V	S	I	N	G	H

IMPLEMENTATION

In Phase-1 the palette of colors is used to select a password for the document/message to be sent. The combination of Red, Green and Blue makes up a color which will be used for authentication. The first level security is enabled through this mechanism. Each color is going to have a numeric value that ranges from 0 to 255. The combination of values of Red, Green and Blue is going to generate a value which will be password for the destination computer. Thus in Phase-1 security is provided through password which is a strong mechanism hard to crack. The palette scheme used for selection of color is represented below. Phase-1 will be followed by Phase-2 of encryption.

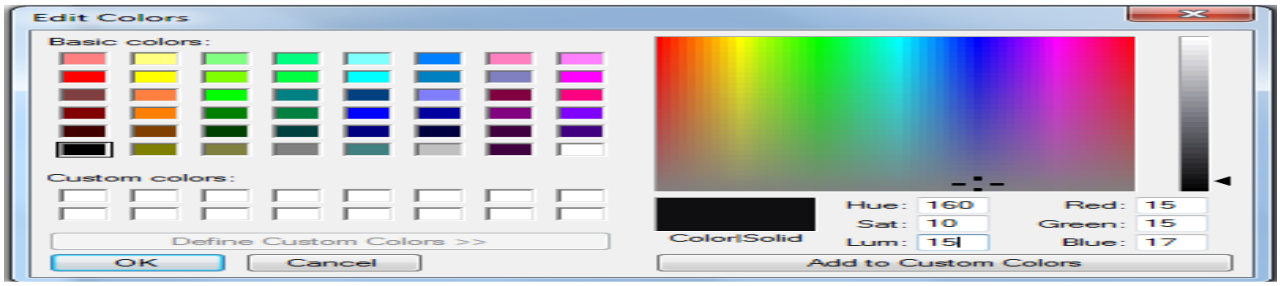
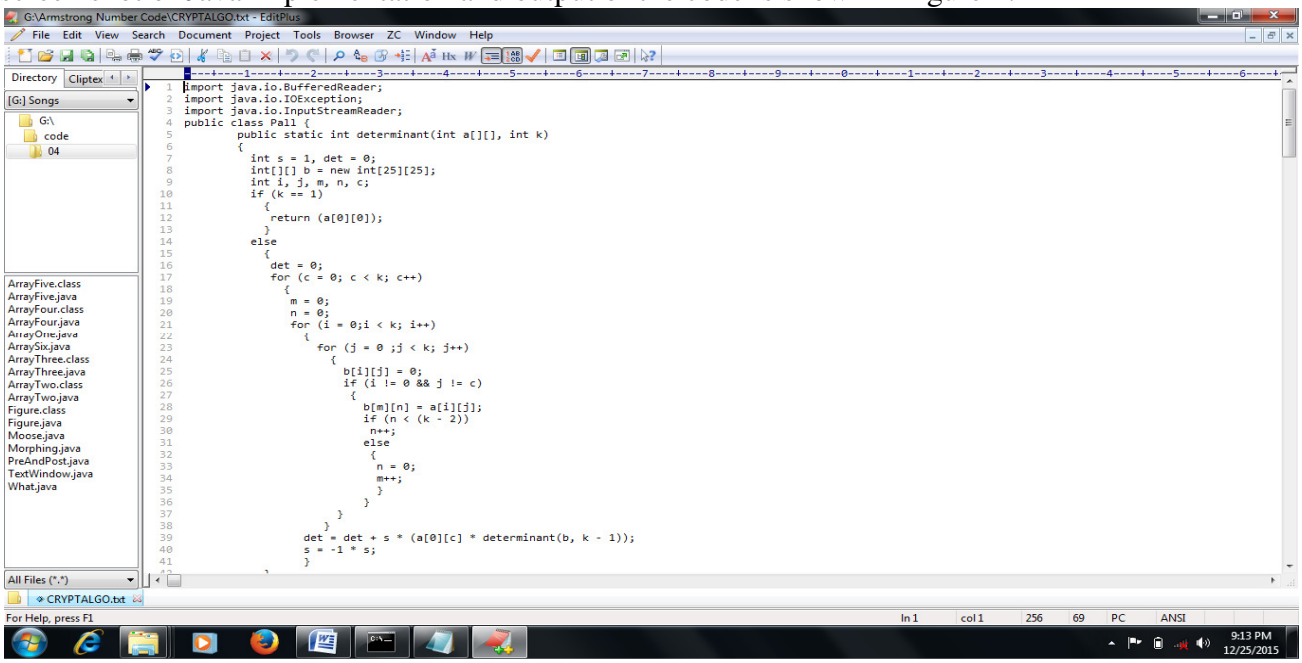


Figure1: Palette Scheme for Selecting Color Password

The implementation of Phase-2 i.e. ARMSTRONG number implementation is made in Java. The screen shot of Java implementation and output of the code is shown in figure 2.




```
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
public class Pall {
        public static int determinant(int a[][], int k)
        {
          int s = 1, det = 0;
          int[][] b = new int[25][25];
          int i, j, m, n, c;
          if (k == 1)
            {
             return (a[0][0]);
            }
          else
            {
             det = 0;
             for (c = 0; c < k; c++)
               {
                 m = 0;
                 n = 0;
                 for (i = 0;i < k; i++)
                   {
                     for (j = 0 ;j < k; j++)
                       {
                         b[i][j] = 0;
                         if (i != 0 && j != c)
                         {
                           b[m][n] = a[i][j];
                           if (n < (k - 2))
                            n++;
                           else
                            {
                             n = 0;
                             m++;
                            }
                         }
                       }
                   }
                det = det + s * (a[0][c] * determinant(b, k - 1));
                s = -1 * s;
                }
```

Figure 2: Implementation of ARMSTRONG Number Code

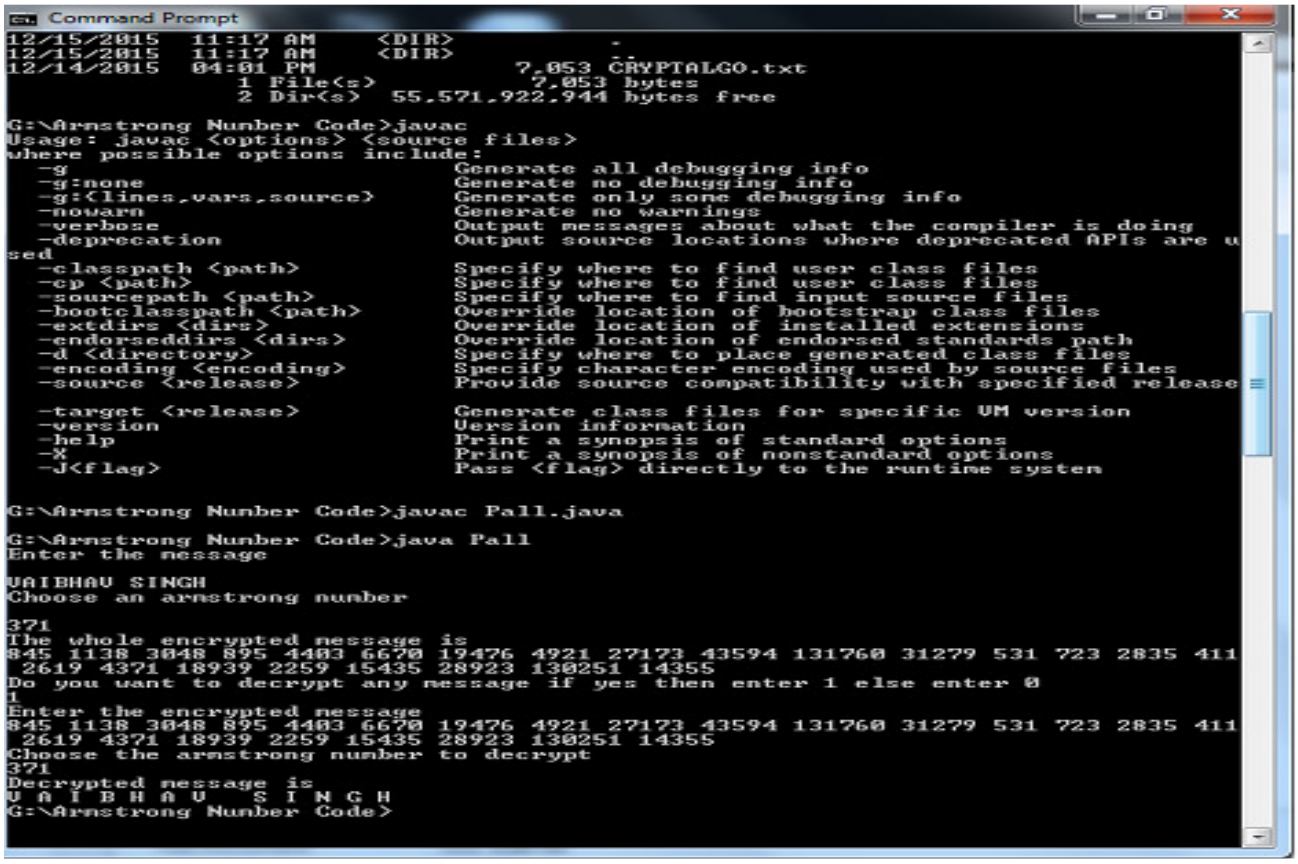


Figure 3: ARMSTRONG Code output implemented in Java

CONCLUSION

The proposed algorithm is a useful method to enable security for the data being transmitted over the network. The color coding technique used as password for providing authentication in Phase-1 is a useful method for providing first level security. Color coding technique is a good mechanism for setting password. Also, the second level security provided through ARMSTRONG number is also a very useful method for finding security to the network data. ARMSTRONG number of Phase-2 suffers from various limitations like there are some cases where the value becomes zero during the process of the calculation and leads to undeterminable result. Also password setting of color also has a range of values which can be cracked by an efficient hacker, who is able to identify that color values are taken as password.

REFERENCES

Singh V.K. and Singh D.K. (2015). Proposing BPN based IDS for security in Cloud, *Proceeding of 10th International Conference on Instrumentation, Electrical and Electronics Engineering (ICIEEE 2015) & 10th International Conference on Cloud Computing Computer Science and Advances In Information Technology (ICCCCIT 2015), TROI India*, Delhi , India, 1-7.

Singh V.K., Dubey V. and Singh A.K. (2010). Proposing Data Mining as an Efficient Technique for Solving Frauds in Digital data. *Proceeding of 1st International Conference on Intelligent Information Systems and Management*, IISM'10, RVS College of Engineering and Technology, Coimbatore, Tamilnadu, India, 1-4.

Singh V.K. and Singh A.K. (2010). Dual Level Digital Watermarking for Images. *Proceeding of International Conference on Methods and Models in Sciences and Technology (ICM2ST-10), Published by American Institute of Physics(AIP)*, Chandigarh, India, 284-287.

Singh V.K. and Singh D.K. (2015). Secured Data Packet Transmission by using the RGB color coding technique for computer network. *Proceeding of 11th International Conference on Computer Science and Information Technology-ICCIT 2015 & 11th International Conference on Innovation in Electrical and Electronics Engineering- ICIEEE 2015*, Pune, India, 1-5.

Singh V.K. and Singh D.K. (2015). A new approach towards Security: Multiple Digital Signature. Proceeding of Sustainable- Key to Business, Environmental, Linguistic, Scientific and Technological Fields, National Conference VIBHAVAT-2, RJS First Grade College, Bengaluru, Karnataka, India.