Security of Data Based on Color and Armstrong Number

Puja Maruti Lad
Computer Science and Engineering,Pune University, H.S.B.P.V.T'S COE Kashti, Tal:-Shrigonda,Dist:-Ahmednagar, Maharashtra,India.

Yallawa Shivaji Vhankade
Computer Science and Engineering,Pune University, H.S.B.P.V.T'S COE Kashti, Tal:-Shrigonda,Dist:-Ahmednagar, Maharashtra,India.

Ashwini Jagannath Khandagale
Computer Science and Engineering,Pune University, H.S.B.P.V.T'S COE Kashti, Tal:-Shrigonda,Dist:-Ahmednagar, Maharashtra,India.

Prajakta Ram Bhalerao
Computer Science and Engineering,Pune University, H.S.B.P.V.T'S COE Kashti, Tal:-Shrigonda,Dist:-Ahmednagar, Maharashtra,India.

Abstract – Today, the main issue is the information security. By the information security, Confidentiality, respectability, non-disavowal, verification, for the most part involves. Cryptography is the widespread procedure for contribute certainty of transmitted information. To give security and encryption of the information by utilizing a color as the password and key including whole numbers that I have executed a novel methodology. With the assistance of three arrangement of keys secure information transmission are given as essential security component acted by the color consequently giving confirmation.

Index Terms – Information, Security, Cryptography.

1. INTRODUCTION

Today, to make secure information transmission there utilizations diverse techniques. One of the strategies is Cryptography. In Cryptography, the basic information is changed over into garbled structure and again get back it in unique structure utilizing the encryption and decryption process. In existing framework is the Security Using whole Numbers with Color. In that the initial step is for every receiver approve a unique color. Set of three key values represented with every color. For instance In RGB design (238, 58,140) is represented by violet red color. An arrangement of three key values are appoint to every receiver in the following step. Information is available At Sender and Receiver closes the. To which required receiver the information will need to send the sender think about it. Along these lines, the recipient's special color is utilized as the secret key.

In the color esteem the set which has three key values are included and encrypted at the sender's side. This encoded color use as a secret key. The genuine information is encoded Using whole numbers. The receiver known his own color and key values. The key values are subtracted from genuine color esteem at the receiver's side and decode the encrypted color. At that point receiver send that unencrypted color to the sender for coordinating. Utilizing whole number the genuine information unencrypted just if that color match with senders color.

Cryptography, is worried with keeping correspondences private. The encryption is the transforming the information into indecipherable structure. Its intension is to keep the data hidden from anybody which gives surety of protection. The decoding is the opposite procedure of encryption; it is get the original data from the encoded data. For both of these procedures the secret data are utilized, typically called as a key. The plain content is the information to be encrypted. The encrypted information is acquired as a consequence of encryption procedure is called as cipher content. The same key is utilized for encryption and in addition decryption, there might be diverse keys are utilized for encryption and decoding relying upon the encryption component.

In this system the initial step is allocate a one of a kind color for every receiver. With every color an arrangement of three key values are represented. i. e. RGB design as (238, 58,140) is represented by violet red color. Appoint a three key values' set to every receiver in the following step.

The sender is thought about the required receiver which needs to send the information. So that the receiver's interesting color utilized as a password. The arrangement of three color values are included the first color values and which are encoded at the sender's side. At that point this encoded color

is use as a password. The real information is encrypted using whole numbers.

The own color other key values are known not receiver, at the recipient's side. To unscramble the encrypted color by sender Receiver subtract the key values from the color values. At that point for match send that unencrypted color to the sender. The genuine information can be decoded by utilizing the whole number just if the color get matched at sender side. The information giving confirmation, to get the surety of some re-security utilize the color as a password. This is on account of when the colors at these recipient's side match with one another then just the real information could be gotten to.

1.1. Types of Cryptographic Algorithms

Depending upon the quantity of keys are possessed for encryption and decryption the cryptographic algorithm characterized by a few ways. They are arranged, and facilitate depict by their application, there are three sorts of algorithm which are:

1.1.1. Secret Key Cryptography (SKC)

In this algorithm utilizes a single key for both encoding and decoding.

Ex. Advanced Encryption Standard (AES), Data Encryption Standard (DES)

1.1.2. Public Key Cryptography (PKC)

In this algorithm, for encryption and decryption utilizes distinctive keys.

Ex. RSA (Rivest, Shamir, Adleman) algorithm.

1.1.3. Hash Functions:

To irreversibly "scramble" data utilizes a numerical change.

Ex. MD (Message Digest) algorithm.

Fig 1. Secrete key (symmetric) cryptography

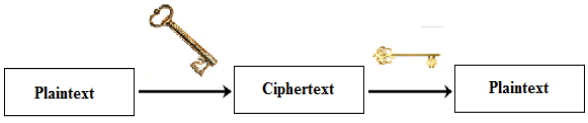

Fig 2. Public key (asymmetric) cryptography

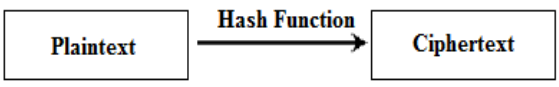

Fig 3. Hash Function (One way cryptography)

1.2. RGB Color Format

The primary colors are red Green and Blue. What's more, by the combination of these three essential colors any color is shaped. Which are in settled amounts. In a PC RGB representation the color is put away as Red, Green and Blue by representing to their amounts. In the PC for putting away the picture in PDF, JPEG or BMP groups, the RGB representation is use. By every pixel the Values for Red, Green and blue is represented to. Subsequently any color can be interestingly represented to as estimations of Red, Green and Blue in the three dimensional RGB 3D shape.

In the RGB color model to create different colors, the estimations of Red, Green and Blue are consolidation together in various ways. By utilizing helpful permutation of Red, Green and Blue intensities numerous colors can be represented to. Normally, 24 bits are utilized to store a color pixel in which 8 bits each for red, green and blue. For every tone, every one of these colors are available in the scope of 256 conceivable values. 16 777 216 (256^ 3 or 2^24). With this framework, different mixes of force and shade can be indicated.

2. RELATED WORK

The utilization of public key cryptography is tireless and security regions in the data assurance. The prime numbers uses by public key cryptography algorithm comprehensively because the prime numbers are a vital part of the general public key frameworks. Utilizing two principle steps this method guarantees that information exchange can be performed with assurance. In that change over the information into ASCII structure is initial step, then by including it with the whole numbers digits. Second step is to era of the required encrypted information, encode it utilizing a framework. The following procedure gets to be troublesome with this system. Since by various ways the whole number is utilized as a part of every stride. Three unique keys are utilized which are whole numbers, key values included with the colors and the colors. Information can be recovered just if all the three key values alongside this strategy is known. Utilizing Simple encryption and decryption procedures the Encoding and interpreting the real information include. Be that as it may, in this proposed system, the password itself is encoded to give most extreme security to getting to the introductory data. Whole numbers and colors are utilized as a part of this method. The sender is thought about the obliged receiver to whom the message must be sent, [1], [5]-[7].

3. PORPOSED MODELLING

In the existing system for including keys there is the utilization of prime number and like. At that point the further stride ahead in that we utilize whole numbers and color. We additionally utilize a permutation of stage and substitution techniques for surety of data security.

3.1. System Architecture

The substitution procedure is for each characters we allocate the ASCII proportionate. The change procedure is finished Using matrices and whole number. The initial step of this method is for every receiver to select an alternate color. Set of three values are represented to with every color. For instance in RGB design as (238, 58,140) is represented to by violet red color. In the following for each receiver relegate an arrangement of three key values.

Common Database Of The Sender	**Date Stored At Each Receiving End**
Receiver A Color-Pink(255, 192, 203) Key- (+10, -5, -5)	Receiver A Color-Pink(255, 192, 203) Key- (+10, -5, -5)
Receiver B Color-Violet red(238, 58, 140) Key- (+15, -7, -8)	Receiver B Color-Violet red(238, 58, 140) Key- (+15, -7, -8)
Receiver C Color-Raspberry(135, 38, 87) Key- (-20, +10, +10)	Receiver C Color-Raspberry(135, 38, 87) Key- (-20, +10, +10)

Table 1. Data at sender and receiver end.

In data about receiver knows not sender. So that the receiver's registered color as a password use. With the arrangement of three key values the first color values are included and afterward encoded at the sender's side. At that point utilize this encrypted color as a password. At that point utilizing whole numbers genuine information is encoded.

The recipient is referred to his own particular color as well as other key values at the receiver's side. At receiver side the receiver unscramble the subtracting so as to shade which is encoded the key values from the color esteem by the sender. At that point it is coordinated with the color which is put away at the sender's database. Just when the color are coordinated the specific data decoded with the assistance of whole numbers, for confirmation utilization of color as a secret key for surety of most extreme security to the data giving. This is on account of in the wake of coordinating the color at sender and recipient's side with one another the secret information could be gotten to.

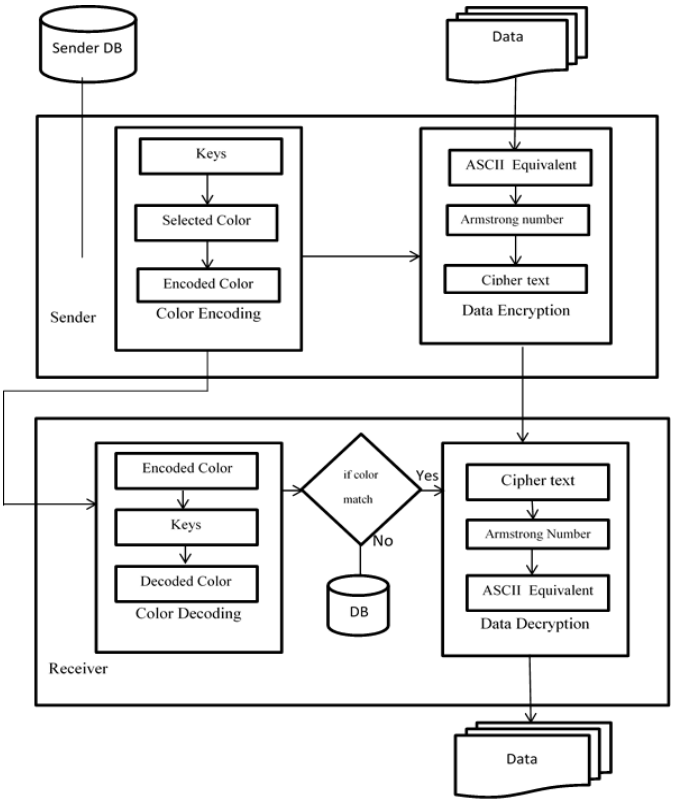

Figure 4. System Architecture

4. RESULTS AND DISCUSSIONS

Figure 6. Sender Login

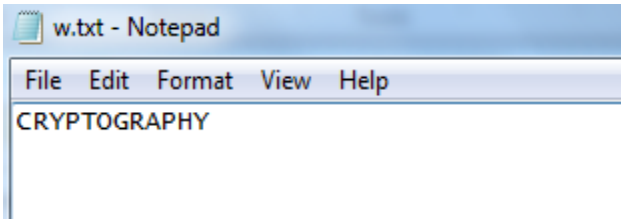

Figure 7. Text of file before encryption

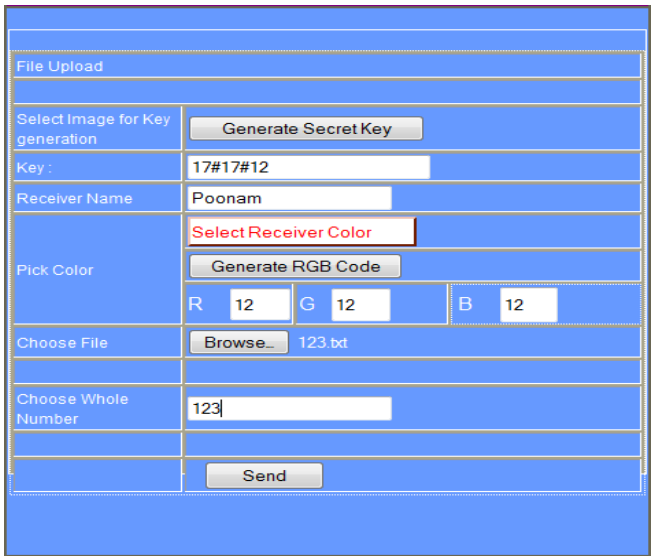

Figure 8. Key generation and file uploading

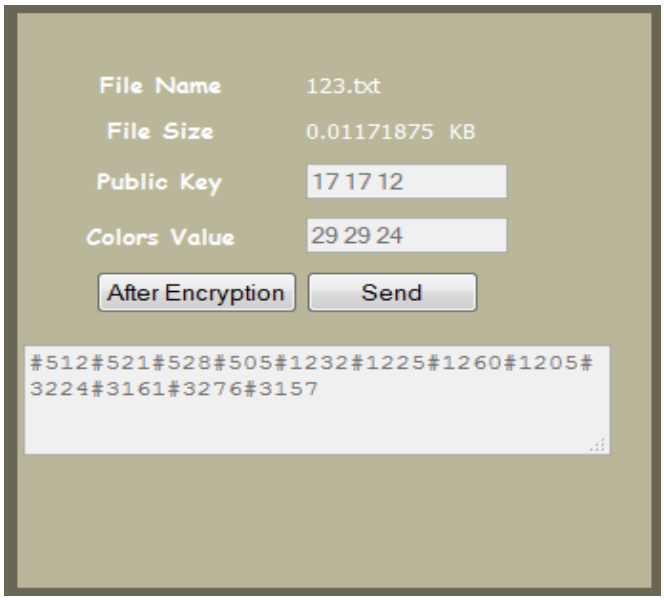

Figure9. Encrypted text

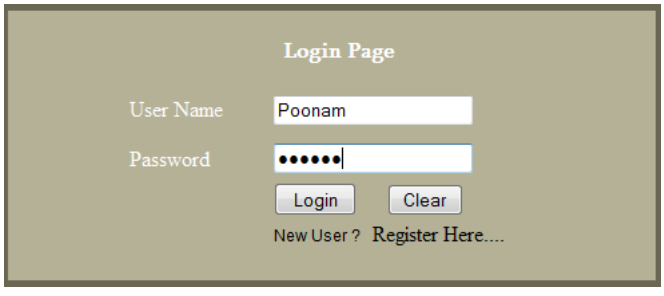

Figure 10. Receiver login

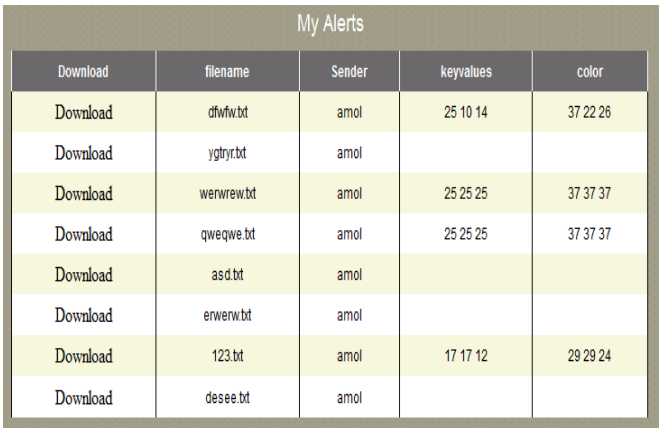

Figure 11. Receiver's messages

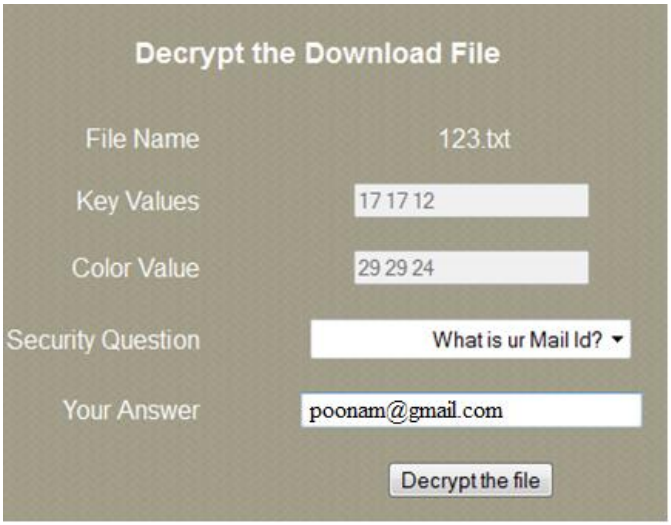

Figure 12. Color verification for file download

Figure 13. Receiver's unique color

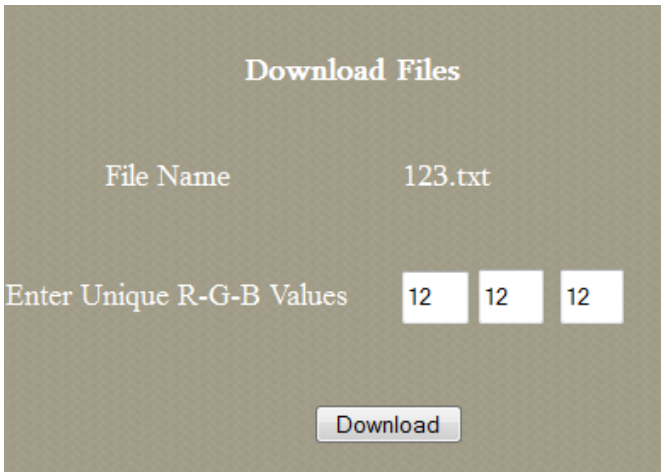

Figure 14. File decryption

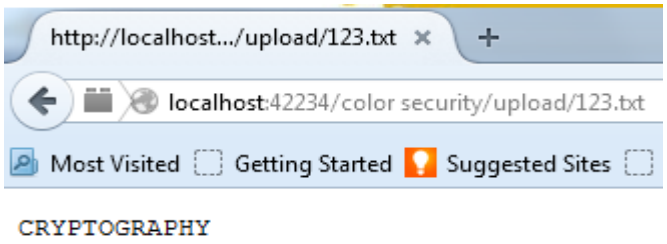

Figure 15. Decrypted file

5. CONCLUSION

In military, there is more significance for security of information for that the above blend of open key and discharge key cryptography can be connected. This system gives more security when the length of the key of the Whole numbers increment. In this manner by the utilization Whole numbers, extra arrangement of key values and hues are utilized. In this method the information is convey safely is the surety of this system and that just approved people groups can get to it.

REFERENCES

[1] S. Pavithra Deepa, S. Kannimuthu, V. Keerthika., "Security Using Colors and Armstrong Numbers", Proceedings of the National Conference on Innovations in Emerging Technology-2011. India.17 & 18 February, 2011.pp.157-160.
[2] Gordon L. Miller and Mary T. Whalen, "Armstrong Numbers", University of Wisconsin, Stevens Point, WI 54481 (Submitted October 1990).
[3] S.Belose, M.Malekar , G.Dharmawat, "Data Security Using Armstrong Numbers", International Journal of Emerging Technology and Advanced Engineering. Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 4, April 2012).
[4] M.F.Armstrong "A brief introduction to Armstrong Numbers" .
[5] Chavan Satish, Lokhande Yogesh, Shinde Pravin, Yewale Sandeep, Sardeshpande S. A, "Secure Email using Colors and Armstrong Numbers over web services", International Journal of Research in Computer Engineering and Information Technology VOLUME 1 No. 2.
[6] M.Renuga Devi, S.Christobel Diana, "Enhancing Security in Message Passing Between Sender and Receiver Using Colors and Armstrong Numbers", International Conference on Computing and Control Engineering(ICCCE 2012), 12 & 13 April, 2012
[7] G.Ananthlakshmi, S.Ramamoorthy "A Multilevel Encryption Scheme for Secure Network Data Transfer". International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.
[8] Atul Kahate, "Cryptography and Network Security", Tata McGraw Hill Publications
[9] http://aix1.uottawa.ca/~jkhoury/cryptography.htm
[10] http://mathworld.wolfram.com/UnimodularMatrix.html

Authors

PUJA M. LAD perceiving the B.E. degree in Computer Science and Engineering from the University of Pune, Ahmednager, Maharashtra, in 2015-16.

ASHWINI J.KHANDAGALE perceiving the B.E. degree in Computer Science and Engineering from the University of Pune, Ahmednager, Maharashtra, in 2015-16.

YALLAWA S.VHANKADE perceiving the B.E. degree in Computer Science and Engineering from the University of Pune, Ahmednager, Maharashtra, in 2015-16.

PRAJAKTA R.BHALERAO perceiving the B.E. degree in Computer Science and Engineering from the University of Pune, Ahmednager, Maharashtra, in 2015-16.