Secure Data Communication using AES Algorithm, Palindrome Number & Color Code

Prof. Manoj Dhande, Akshaya Sawant, Nidhi Pandey, Pooja Sahu
Computer Science Engineering, Shah & Anchor Kutchhi Engineering College
Mumbai, India
manoj.dhande@gmail.com, akshayagsawant@gmail.com, nidhi_440@yahoo.com, poojasahu62818@gmail.com

***Abstract*— Encryption is most effective way to achieve data security. This is done by converting the data into cipher text. The existing way of doing this was using Armstrong number and prime number. Since there are few Armstrong numbers therefore a crypt-analyst can easily find the key. In this paper, we are proposing a new encryption technique that uses AES algorithm using color code and palindrome numbers for encrypting any type of file which provides more security than other approach. This paper gives a technique to send data over the network in set of three keys (palindrome number, alphanumeric random key and ASCII value of color code). Normally a crypt-analyst can easily find out the key however in this approach a mixture of palindrome number and color code which is used for encrypting the data. In the same way, decryption will also be done at receiver's side by using inverse of encryption process.

Keywords- *Palindrome number; Cryptography; Color code; Unique Alphanumeric key; AES Algorithm*

*****

I. Introduction

Over the Internet various communications such as electronic mail or the use of World Wide Web browsers are not secure for sending and receiving information. Information sent by those means may include sensitive personal data which may be intercepted. There is commercial activity going on the Internet and many web sites require the users to fill forms and include sensitive personal information such as telephone numbers, addresses, and credit card information. To be able to do that user would like to have a secure, private communication with the other party. Online users may need private and secure communications for other reasons as well. They may simply not want third parties to browse and read their e-mails or alter their content.

A. Cryptography

Cryptography defined as "the science and study of secret writing," concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers, and other methods, so that only certain people can see the real message. The ability to protect and secure information is vital to the growth of electronic commerce and to the growth of the Internet itself. Many people need or want to use communications and data security in different areas. Banks use encryption methods all around the world to process financial transactions. There are many companies and even shopping malls selling anything from flowers to bottles of wines over the Internet and these transactions are made by the use of credit cards and secure Internet browsers including encryption techniques.

Private key systems use a single key. The single key is used both to encrypt and decrypt the information. Both sides of the transmission need a separate key and the key must be kept secret from. The security of the transmission will depend on how well the key is protected.

In the public key system there are two keys: a public and a private key. Each user has both keys and while the private key must be kept secret the public key is publicly known. Both keys are mathematically related [6].

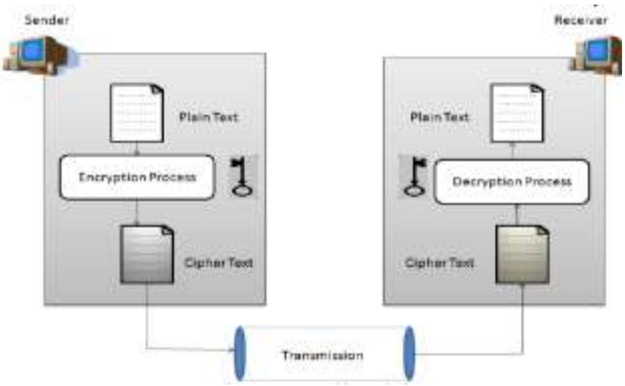

Figure 1[6]

B. RGB representation

Any color is the mixture of three colors RGB (Red, Green and Blue) in present quantities. This is nothing but a RGB representation. Here values for Red, Green and Blue represent each pixel. So any color can be individually represented with the help of three dimensional RGB cube. RGB model uses 24 bits, 8 bits for each color. Hence colors are used as a password for authentication purpose. Then encryption or decryption process takes place[6].

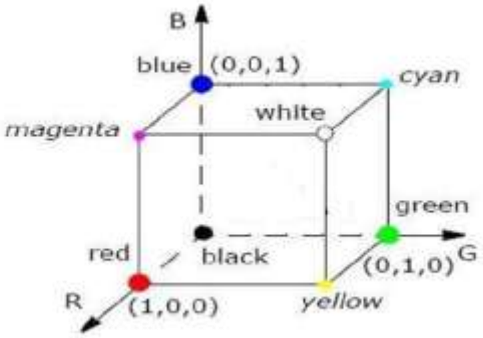

Figure 2

C. Palindrome number

A palindrome is a word or a number or a sequence of words that can be read the same way from either direction, be it forwards or backwards. Hence 151 is an Palindrome number because Reverse(151)=151[2].

D. *Alphanumeric key OR Random key*

Alphanumeric key is a combination of a letters and numbers in particular sequence. We decide here alphanumeric key of size three with two digits and one letter (eg.12A)[2]. Otherwise use random key values for encrypted code generation.

II. EXSISTING SYSTEM

. TABLE I

Sr. No	*Methodology*	*Disadvantage*
1	*Using Armstrong Number as a key for Encryption and Decryption Process*	*Armstrong Numbers are very less in number*
2	*Using Prime Number as a key for Encryption and Decryption Process*	*Prime numbers are very easy to hack by the cryptanalyst*
3	*Using Fibonacci series as a key for Encryption and Decryption Process*	*consume more memory & time.*

III. PROPOSED SYSTEM

Our proposed system follows following steps:

A. *Admin Part*

1) Admin can send any file format to user registered with him secretly.
2) He selects user, then select color code which will be converted into ASCII equivalent and enter some random alphanumeric key values.
3)Then encrypted code i.e.(ASCII equivalent of color code + alphanumeric key values also converted into ASCII) is send to the end user which will be used for authentication of user .
4) Then using this encrypted code system generated palindrome number is generated which will be used as a key in AES algorithm for encryption and decryption purpose.
5) Admin sends mail to user that contains encrypted color code and system generated palindrome number.

B. *User Part:*

1) User Login to the system he check for the mail.
2) To download the file he received from admin, he enters encrypted color code and palindrome number for authentication purpose.
3) If this code matches then only he is able to download the file where decryption using entered palindrome number takes place.
4) User also has an option to reply back to the admin which follows the same process of selecting color code and key values for encryption of the message.
5) This encrypted code generates palindrome number and both of these values are sent to the admin for decryption of sent files.

IV. IMPLEMENTATION

A. *Select Color*

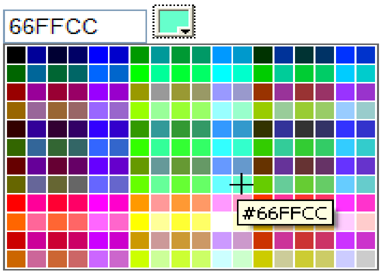

Figure 3

ASCII Equivalent code : (102, 255, 204)

+ Random key values : (156, 259, 369)

Encrypted color code (258, 514, 563)

B. *Generation of palindrome Number*

1. Keep first five(0-5) digits of encrypted color code as it is.
2. Replace last four digits(6-9) By reverse of first four digits.
Original encrypted code: (258514563)
1. String=25851
2. Reverse: 5852
3. Append reverse at end of string we get" 258515852"
Above palindrome number will be used in AES algorithm as key for encryption and decryption purpose.

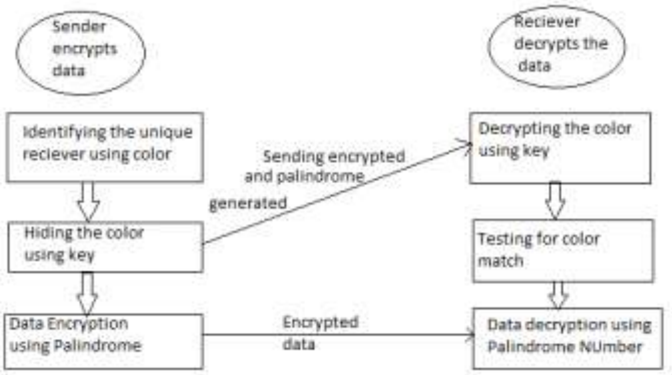
Sender encrypts data
Reciever decrypts the data
Identifying the unique reciever using color
Sending encrypted and palindrome generated
Decrypting the color using key
Hiding the color using key
Testing for color match
Data Encryption using Palindrome
Encrypted data
Data decryption using Palindrome NUmber

Figure 3.System flow Diagram

V. EXISTING SCOPE

This secret sharing approach can be used by companies for sharing of files between the manager and employees in a secret manner. It is a secure approach to file sharing because of the use of color code along with secret key which are used in AES algorithm to encrypt or decrypt the file.

VI. CONCLUSION

This approach achieve security goal such as confidentiality, Authentication, Availability. It achieves Confidentiality because of use of Symmetric encryption algorithm. It achieves Authentication due to use of a color code and random key values for generation of encrypted code which is used in authentication of end user. Despite the use of this sophisticated cryptosystems and random keys, cipher system may be vulnerable if not used properly.

VII. RESULT AND ANALYSIS

We have used the following constraints in our project:
Colors used = 216
Palindrome key = 9digit
KEY=32 Bytes (256 bits)
IV=16bytes (128bits)
We generate key and IV using the derived bytes (Rfc2898DeriveBytes) and the symmetric key.
Considering the above constraints, we have compared the performance of different symmetric algorithms in Table 1 using Crypto++[Crypto++ Library is a free C++ class library of cryptographic schemes. Currently the library consists of the following, some of which are other people's code, repackaged into classes]. We see that AES algorithm performs better regarding time and throughput.

TABLE II

Algorithm	**Megabytes(2^20 bytes) Processed**	**Time Taken**	**MB/Second**
Blowfish	256	3.976	64.386
Rijndael (128-bit key)Standard AES	256	4.196	61.010
Rijndael (192-bit key)	256	4.817	53.145
Rijndael (256-bit key)	256	5.308	48.229
DES	128	5.998	21.340
(3DES)DES-XEX3	128	6.159	20.783
(3DES)DES-EDE3	64	6.499	9.848

For AES of key size = 256 bits, a total of 1.1 x 10^{77} combinations to crack. Such a large combination requires an approximate of 3.31 x 10^{36} years.
Instead of the complications and cost of having an in-house email setup, an increasing number of businesses are turning up to SMTP servers to lower the headaches that comes while managing email activity. Rather than dealing with the email programs aggravations, they can concentrate on the priorities of their companies.

ACKNOWLEDGEMENT

We thank our teachers for their valuable suggestions and guidance that has helped us to accomplish our project work.

REFERENCES

[1] Deepa, S.P. ; Kannimuthu, S. ; Keerthika, V. ; Year 2011 Armstrong numbers, Innovations in Emerging Technology (NCOIET), National Conference on IEEE Conference Publication

[2] J Gitanjali ,Dr.N.Jeyanthi, C.Ranichandra, M.Pounambal ASCII Based Cryptography Using Unique ID, Matrix Multiplication and Palindrome Number.

[3] 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

[4] Aditya Rayarapu et al, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 433-435

[5] Proceedings of the National Conference on Innovations in Emerging Technology-2011 Kongu Engineering College, Perundurai, Erode, Tamilnadu, India.17 & 18 February, 2011.pp.157-160.

[6] Gayatri Kulkarni , Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav, " Message Security Using Armstrong Numbers and Authentication Using Colors", International Journal of Advanced Research in Computer Science and Software Engineering(Volume 4, Issue 1, January 2014 ISSN: 2277 128X).

[7] 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

[8] SarmisthaSaha, A.V.D.N.Murthy, P.SureshBabu"Message Encryption Using Enhanced Palindrome Number"IJDCST @ Nov-Dec, Issue- V-3, I-1, SW-070ISSN-2320-7884 (Online)

[9] Shaify Kansal, Meenakshi Mittal"Performance evaluation of various symmetric encryption algorithms"2014 International Conference on Parallel, Distributed and Grid Computing.