IJDCST @ Nov-Dec, Issue- V-3, I-1, SW-070
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Message Encryption Using Enhanced Palindrome Number

SarmisthaSaha, M.Tech student, A.V.D.N.Murthy, M.C.A, M.Tech, P.SureshBabu,B.Tech, M.E.

Dept. of CSE, KAUSHIK College of Engineering, Gambheeram, Visakhapatnam, A.P, India

Abstract: Technology is constantly improving and has limited shell life. The longer it takes to procure and develop a solution – the less useful the end results. Therefore it makes it all the more important bet on technologies which have exhibited robustness, scalability, support and easier inter –operability. This paper provides a technique for message security in which palindrome number is used for encryption message. Colour is important in authentication process as it acts as a password. Using this technique message can be protected from on-line cyber crime and accessible to an authorized individual when required.

Keywords: Message security, Palindrome numbers ,Authentication, Colours

I INTRODUCTION

Computer security rests on confidentiality, integrity and availability. The interpretations of these three aspects vary, as do the contexts in which they arise. The interpretation of an aspect in a given environment is dictated by the needs of the individuals, customs and laws of the particular organization. In real world, secure data transmission is really difficult because of hackers. Cryptography is the universal technique consisting of encryption and decryption processes that provides us secured data transmission. Encryption and Decryption require a secret entity referred to as a key. The statement

X →Y : { Z } k means that entity X sends entity Y a message Z enciphered with key k

The same or different key might be used for encryption and decryption depending on the situation. Here, we use same keys for both encryption and decryption.

COLOUR MODEL REPRESENTATION:

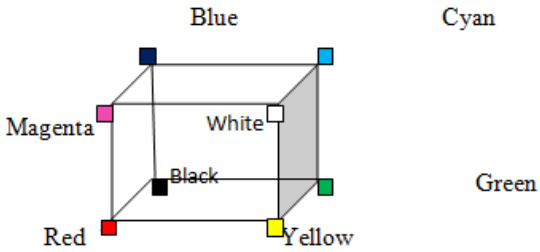

Fig. 1 Colour Cube (RGB)

PALINDROME NUMBER: A palindrome number is an n-digit number which has the same value of its reverse. e.g. 131.

II CRYPTOGRAPHY

The word ***cryptography*** comes from two Greek words meaning "secret writing" and is the art and science of concealing meaning. Crypto analysis is the

breaking of codes. The basic component of the cryptography is a cryptosystem. A ***crypyto system is a 5-tuple(E,D,M,K,C)*** where M is set of plaintexts, K the set of keys (***private or public***) ,C is the set of cipher texts , **E : M x K →C** is the set of ciphering functions, and **D : C x K -> M** is the set of deciphering functions.

III LITERATURE SURVEY

The use of public-key cryptography is persistent in the information protection. Public key cryptography algorithms utilize prime numbers broadly because prime numbers are a crucial part of the public key systems. Given a set K of potential keys, the probability of a key being guessed is at a minimum when the key is selected at random number between $|K| - 1$. Typically many keys are required, so a sequence of random numbers is needed. A sequence of cryptographically random numbers is a sequence of numbers $n_1, n_2, n_3, \ldots$ such that for any positive integer k, an observer cannot predict n_k even if $n_1, n_2, n_3 \ldots n_k - 1$ are known.

This technique ensures that using following steps data transfer can be performed with protection.

i) Convert data into ASCII form
ii) Add with the digits of palindrome number

iii)Encode using a matrix to generate the required encrypted data

Here k=3,

a)Colour Key

b)General Key value added with Colours

c) Palindrome number.

Data can be retrieved only if all the three key values associated with this technique is known

IV. EXISTING SYSTEM

There are many algorithms for encryption and decryption process like AES,DES,RSA in which encryption is done with the help of substitutions and transformations on the plaintext.

It uses prime numbers for encryption process.

A. Cryptography using secret key(SKC) : Secret single key is used for both encryption and decryption.

It includes Data encryption standard(DES) and Advanced Encryption Standard(AES)

B. Cryptography using Public Key(PKC): In this method two different keys are used ,one is for

encryption and another is for decryption.eg. RSA algorithm.

C. Hash Functions : In this method a mathematical transformation is used to encrypt data which is

Irreversible .e.g. Message Digest (MD) algorithm.

V. PROPOSED SYSTEM

In proposed system Palindrome numbers increased by 1 are used for encryption purpose while existing

system uses prime number and armstrong number.There are N number of receivers to whom data to be sent.Initially,each receiver is assigned a particular color value. Sender should identify the particular receiver by the preassigned colour associated with it.Our proposed system follows following steps:

i) Encryption of colour is done by adding key values to the original colour values at sender's side.This encrypted colour acts as a password.

ii) Data is encrypted using palindrome numbers enhanced by 1.

iii) Decryption of colour takes place at the receiver's side when the receiver enter it's private key.

iv) The decrypted colour is then matched with the colour assigned by sender.

v) ASCII equivalent of the data added with the palindrome number is used in matrix format(Here matrix M).

vi) Encoding matrix has been formed(Here matrix N).

vii) Cross Product of two matrices (NxM) gives rise to encrypted data(cited in step -6).

viii) At last decryption process starts (Here from step- 6) and process ends at step-10.

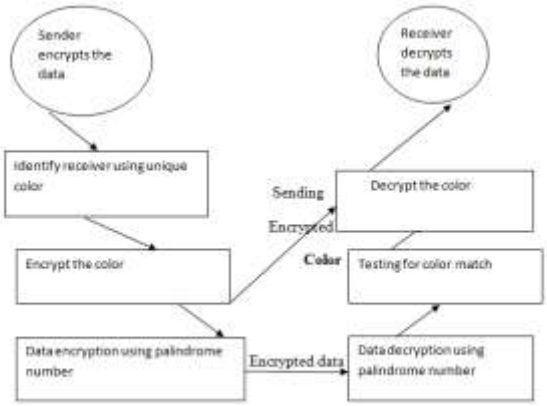

Figure Layout of proposed technique

Step-1: Color Encryption: Sender is aware about receiver's color e.g. purple (128,0,128).Let the

Key values to be added with this colour value be (10,-3,-2).

128 0 128

10 -3 -2

This new colour value(138,-3,126) acts as a password.

Step -2 : Data Encryption starts here.

Let data to be transmitted is "VICKYHI-TECH".

ASCII equivalent of the above characters are as follows :

V I C K Y H I - T E C H

86 73 67 75 89 72 73 45 84 69 67 72

\+ 1 3 2 1 9 4 1 27 8 1 3 2 (Adding Palindrome number)

87 76 69 76 98 76 74 72 92 70 70 74 (Palindrome number added data)

Step -3 : Convert the above Palindrome added data into matrix(M) format

$$\text{Matrix M} = \begin{pmatrix} 87 & 76 & 74 & 70 \\ 76 & 98 & 72 & 70 \\ 69 & 76 & 92 & 74 \end{pmatrix}$$

Step -4 : Encoding matrix(N) is as follows

$$\text{Matrix N} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 9 & 4 \\ 1 & 27 & 8 \end{pmatrix}$$

Step -5 : Taking cross-product of above two matrices(N x M),we get derived matrix (P) as follows :

Matrix P = N x M

$$\begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 87 & 76 & 74 & 70 \\ 76 & 98 & 72 & 70 \\ 69 & 76 & 92 & 74 \end{pmatrix}$$

Matrix P = 1 9 4 X

1 27 8

$$= \begin{pmatrix} 453 & 522 & 474 & 428 \\ 1047 & 1262 & 1090 & 996 \\ 2691 & 3330 & 2754 & 2552 \end{pmatrix}$$

Now the encrypted data is 453, 1047, 2691, 522, 1262, 3330, 474, 1090, 2754, 428, 996, 2552

Step – 6 : Decryption process starts here by authenticating the receiver .

138 -3 126

\- 10 -3 -2

128 0 128

Here key value is subtracted from the pre assigned password.

Step -7: Decryption of the encrypted data to get the original sent data is as follows:

Now decoded matrix (Q) = Inverse of encoded matrix (N) = N^{-1}

$$= \begin{pmatrix} 3 & -5/2 & 1/2 \\ -1/3 & -1/2 & 1/6 \\ -3/2 & 2 & -1/2 \end{pmatrix}$$

Step -8 : Multiplying the decoded matrix with the encrypted data :

$$Q \times P = \begin{pmatrix} 3 & -5/2 & 1/2 \\ -1/3 & -1/2 & 1/6 \\ -3/2 & 2 & -1/2 \end{pmatrix} X \begin{pmatrix} 453 & 522 & 474 & 428 \\ 1047 & 1262 & 1090 & 996 \\ 2691 & 3330 & 2754 & 2552 \end{pmatrix}$$

$$= \begin{pmatrix} 87 & 76 & 74 & 70 \\ 76 & 98 & 72 & 70 \\ 69 & 76 & 92 & 74 \end{pmatrix}$$

Step -9: Now transform the above result as given below:

87 76 69 76 98 76 74 72 92 70 70 74

Step -10: Subtracting with the digits of the palindrome number which is enhanced by 1

87 76 69 76 98 76 74 72 92 70 70 74

-1 3 2 1 9 4 1 27 8 1 3 2

---

86 73 67 75 89 72 73 45 84 69 67 72 (ASCII equivalent of original data)

VI. CONCLUSION

Despite the use of this sophisticated cryptosystems and random keys, cipher system may provide an adequate security if not used properly. Even though our proposed system uses three key values i.e. colour , receiver's key and palindrome number enhanced by 1, we may predict that it gives very secured approach to send data but in the real world there are so many hackers who can able to break this sophisticated method. But no doubt this present approach is still worthy enough to sent data.In future we will try to enhance more sophisticated method.

ACKNOWLEDGEMENT

It is my pleasure to express our sincere gratitude to KAUSHIK ENGINEERING COLLEGE for providing us an opportunity to do our work on paper. We sincerely thank to our project guide Mr. A.V.D.N MURTHY, Asst. Professor and course coordinator Mr. Suresh Babu for guiding and encouraging in carrying out this paper work.

P.Suresh Babu completed his B.Tech and M.E. in Computer Science and Engineering. He is currently working as Associate professor of Department of computer science and engineering at Kaushik College of engineering, JNTUK University. He is having industrial experience of 4 years and teaching experience of 15 years. His areas of interest include Artificial intelligence, Neural Networks, Cryptography & Network security, Compiler Design and Advanced Data Structures.

teaching experience of 7 years. His areas of interest include Data mining, Image Processing, Cryptography & Network security, Computer Networks and Operating Systems.

A.V.D.N.MURTHY completed his MCA and M..Tech. in Computer Science and Engineering. He is currently working as Assistant Professor of Department of Computer Science and Engineering at Kaushik College Of Engineering, affiliated to JNTUK University. He is having industrial experience of 1.2 years and

REFERENCES

1. http://www.aix1.uottawa.ca/~jkhoury/cryptography.html
2. http ://www.scribd.com/doc/29422982/Data-Compression-and-Enciding-Using-Col
3. “Cryptography and Network Security” By Atul Kahate TMH
4. Higher Algebra(Abstract and Linear) – S.K.Mapa , Sarat Book House