International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.4., 2015
(July-Aug)

RESEARCH ARTICLE

ISSN: 2321-7758

ASCII PRIMARILY BASED CRYPTOGRAPHY VICTIMIZATION DISTINCTIVE, MATRIX OPERATION AND PALINDROME RANGE

UBHAD SANKET A[1*], Prof. CHAUBEY NILESH[2], Prof. DUBEY SHYAM P[3].

[1.]M.Tech Scholar, NCET, Nagpur,

[2.]Asst. Prof. Dept. of Electronics, MIET, Gondia,

[3.]Asst. Prof. Dept. of CSE, NCET, Nagpur

UBHAD SANKET A

ABSTRACT

Cryptography is only thanks to succeed information security. this is often done by changing the info into cipher text. The existing manner of doing this was victimization Armstrong range. Since there square measure few Armstrong numbers so a crypt-analyst will easily realize the key. During this paper, we tend to square measure proposing a brand new algorithm for cryptography technique, UPMM rule, which is applied on computer code worth of knowledge. Computer code values square measure encrypted using a key involving word numbers and distinctive alphanumeric id,that is additionally reborn into computer code worth to provide authentication over the network. This paper offers a technique to send information over the network in set of 3 keys. Normally a crypt-analyst will simply determine the key but in this approach a combination of word range and matrix multiplication is employed for encrypting the info. within the same manner decryption will be done at receiver's facet by victimization inverse of encoding matrix.

Keywords-ASCII values, Palindrome number, Cryptography, Matrix multiplication, distinctive Alphanumeric Id

I. INTRODUCTION

The drawback of existing strategies used for cryptography of text is finished directly over the text. These strategies uses prime range or Armstrong number as key that was simply break by crypt-analyst. Excluding this no authentication facility was provided to create the info safer that is necessary whereas causing confidential information like credit cards transactions, banking transactions and social insurance numbers.

The solution to higher than downside is that by providing a singular alphanumeric id to receiver which is able to be acknowledged by sender. This id is reborn into various computer code worth and set of random range is further to those computer code values.

The summation of this resultant computer code values is employed to come up with palindrome range. The text that should be send is additionally converted into computer code worth so encrypted victimization the palindrome range generated higher than. Computer code values of check square measure converted by creating it a matrix so multiplying it by Encoding matrix.

Types of Keys

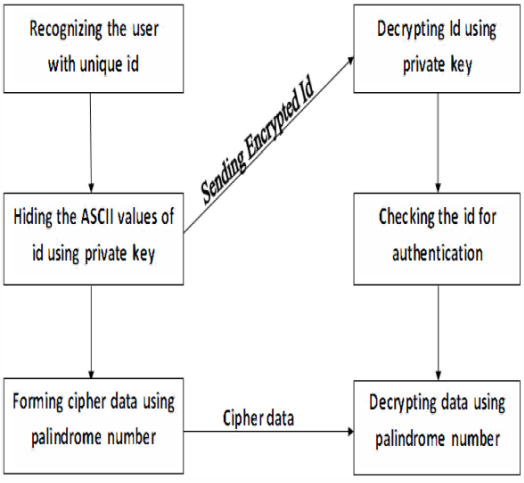
Private Key: Private Key cryptography contains identical key for sender and therefore the receiver. The sender sends the key alongside the info for receiver to decipher the data victimization identical key.

Public Key: Public key cryptography can used each non-public and public key. Public key are send to any

or all approved user which may be enabled for all and one non-public key which can be acknowledged by solely receiver. Public key's used for cryptography and personal key for cryptography.

II. PLANNED TECHNIQUE

A. Introduction: The objective of this paper is to propose a brand new technique of cryptography. It changes the info into its various computer code values so converts these computer code values to cipher text using the word range. The strategy additionally uses matrix multiplication that makes information safer from obtaining Encrypted by intruders. Apart from this it additionally offer authentication by a singular alphanumeric id that is provide to every receiver. This id acts as private key at the start each receiver is given AN id and sender database has of these ids keep in it. Ids ought to have 3 alphabets and one range. Whereas causing information, set of 4 values is generated at sender facet which is further to ASCII equivalent of receiver id. The summation of those values once addition is then accustomed generate a word number. At the receiver facet encrypted information is received alongside key and random range set. This key's then decrypted and compared with receiver id. Original information is encrypted providing those two id matches. Recognizing the user Decrypting Id victimization with distinctive id and non-public key hiding the computer code values of checking the id for id victimization non-public key authentication. Forming cipher information victimization Cipher information Decrypting information victimization palindrome range word range.



Outline of Proposed Method

B. ILLUSTRATION

1) Encryption: For example allow us to assume that we want to send the info to receiver Z. Z is allotted with an alphabetical key (say SRPI). Its computer code equivalent is (83 eighty two eighty 49). Suppose random key generated be (8 7 14 11).

Sender should know about the receiver id. The random key is then added to this id assigned to receiver.

S R P I
83 82 80 49
8 7 14 11
---
91 89 94 60

Step2: Creating a palindrome number

Summation of these encrypted key id done and next palindrome number to sum is calculated.

91 + 89 + 94 + 60 = 334

Palindrome number nearest to 334 is 343. This number is used to encrypt the actual data.

Step3: Encoding matrix

Let digits of palindrome number is denoted by i, j and k. These values are used as first row elements of matrix.

i=3 j=4 k=3

Second and third rows elements of matrix is formed using following way

(i+l)*3 (j+3)*4 (k+5)*3

$$A = \begin{vmatrix} 3 & 4 & 3 \\ 12 & 28 & 24 \\ 39 & 124 & 87 \end{vmatrix}$$

Step4: cryptography of knowledge

Let the info to be encrypted be ability.

This information is 1st reborn into computer code values.

I N T E R O P E R A B I L I T Y

73 78 84 69 82 79 80 69 82 65 66 73 76 73 84 89

This matrix is represented in matrix form as follow.

$$B = \begin{vmatrix} 73 & 78 & 84 & 69 & 82 \\ 79 & 80 & 82 & 65 & 66 \\ 73 & 76 & 73 & 84 & 89 \end{vmatrix}$$

Step5: Now adding column elements of B with row elements of A

Step6: now multiplying the two matrices (A *C) .

$$\begin{vmatrix} 73+3 & 78+12 & 84+39 & 69+3 & 82+12 \\ 79+4 & 80+28 & 82+124 & 65+4 & 66+28 \\ 73+3 & 76+24 & 73+87 & 84+3 & 89+24 \end{vmatrix}$$

$$C= \begin{vmatrix} 76 & 90 & 123 & 72 & 94 \\ 83 & 108 & 206 & 69 & 94 \\ 76 & 100 & 160 & 87 & 113 \end{vmatrix}$$

$$D= \begin{vmatrix} 245 & 308 & 499 & 238 & 311 \\ 299 & 362 & 553 & 292 & 365 \\ 485 & 548 & 739 & 478 & 551 \end{vmatrix}$$

The cipher text which is send over the network is 245, 308, 499, 238, 311, 299, 362, 553, 292, 365, 485, 548, 739, 478, and 551

2) Decryption

Step 1: *valedictory receiver*

On receiving the encrypted information alongside the key first the receiver is documented. It's done by subtracting random numbers (generated by sender) from the key.

91 89 94 60 (received data)
\- 8 7 14 11 (key)
---
83 82 80 49
S R P 1

The resultant is then reborn back to id and compared with id of receiver. cryptography of knowledge is finished providing receiver is valid by victimization following steps

Step 2: *Secret writing matrix:*

Encoding matrix is once more created victimization same technique used during encryption. The inverse of this matrix in calculated that is secret writing matrix (say E)

$$1/244 = \begin{vmatrix} -540 & 24 & 12 \\ -108 & 44 & -36 \\ 636 & -136 & 36 \end{vmatrix}$$

Step3: Received data is used to form a matrix

$$F= \begin{vmatrix} 245 & 308 & 499 & 238 & 311 \\ 299 & 362 & 553 & 292 & 365 \\ 485 & 548 & 739 & 478 & 551 \end{vmatrix}$$

Now multiplying secret writing matrix with this matrix we get,

Step 4: obtaining back original information Row of E is subtracted from columns of G and that we get

$$G= \begin{vmatrix} 76 & 90 & 123 & 72 & 94 \\ 83 & 108 & 206 & 69 & 94 \\ 76 & 100 & 160 & 87 & 113 \end{vmatrix}$$

following matrix.

This produces back a matrix that has original information

This produces back a matrix which has original data

$$\begin{vmatrix} 73 & 78 & 84 & 69 & 82 \\ 79 & 80 & 82 & 65 & 66 \\ 73 & 76 & 73 & 84 & 89 \end{vmatrix}$$

Step5: currently remodel the higher than matrix as given below which square measure computer code equivalent of knowledge and so reborn back to characters.

I N T E R O P E R A B I L I T Y
73 78 84 69 82 79 80 69 82 65 66 73 76 73 84 89

III. CONCLUSION

In this technique no new information is further so it becomes difficult to search out however cryptography is finished on the info. Even if the persona non grata get the message, it's powerful for him to rewrite the data since summation of personal key's accustomed generate palindrome range. Then this range is any accustomed produce the cryptography matrix. technique accustomed kind the cryptography matrix is a advanced that makes it troublesome to search out the cryptography matrix and so original information stay secure.

In future this technique will be created secure by victimization different pattern for distribution id to receiver. Formula accustomed form the cryptography matrix will be created a lot of advanced that will create it undetectable by hackers and intruders.

IV. REFERENCES

[1]. Deepa, S.P. ; Kannimuthu, S. ; Keerthika, V. ; Year 20ll Security using colors and Armstrong numbers, Innovations in Emerging Technology (NCOlET), National Conference on lEEE Conference Publication.

[2]. http://www.totse2.com/content.php? 228-Basic-Cryptograpy-with- Matrices.