International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 02, February 2017
www.ijates.com
ijates
ISSN 2348 - 7550

ENCIPHERING USING CANTOR PAIRING FUNCTION AND COMPUTED KEY

M. Hanumanthu[1], T. Mukthar Ahamed[2], V. Siva Kumar[3]

[1,2]Teaching Assistant, Dept.of CSE, YSR Engineering College of YVU, Proddatur, (India)

[3] Student, III CSE, YSR Engineering College of YVU, Proddatur, (India)

ABSTRACT

Now a days the exchange of information electronically faces some issues. This has to be more secure since it takes network as a medium for information transceiving. No one should peep the content or modify the content. With the presentation of web and circulated framework made the data security issue all the more difficult and complex. So data security is an essential viewpoint now a day. Cryptography plays a main role in providing security to the data we assumes to be information that takes web for transmission. Control mechanism provided by cryptography in maintaining system confidentiality prompting to the advancement of more number of commonsense applications to uphold security in system. In the current work they build up a figure which utilizes essential encryption strategies of substitution and transposition alongside utilization of rationale doors to encode the information. In that all traditional methods are used in proposed method we develop a cipher by proposing cantor pairing function.

Keywords: Cantor pairing, Ceaser Cipher, Cryptograhy, Encryption, XNOR.

I INTRODUCTION

The advancement in cryptography is sophisticated in encrypting mechanisms and decoding. Validating our lives in terms of protection is very basic level in day today life [1]. We utilize confirmation all through our regular day to day existences by introducing ourselves with some basic information and switching choices by assenting and imparting in electronic process, electronic systems are required for the process of validation [2]. These strategies are adopted in the systems by the techniques of cryptography. An advanced mark ties a record with holder of a specific mapped key, at the same time a computerized timestamp ties an archive to its formation in a specific time slot [3]. These protected instruments makes utilization in controlling restricted access to area by establishing full security measures, or a compensation for each TV channel view. The area in the world of cryptography incorporates different needs also. By taking a couple of fundamental cryptographically moulded apparatuses, can help in conceivable and fabricating with expound plans for conventions that permit cash payment electronically, in the process of demonstration the data without uncovering itself in proper way, and sharing amount in the manner creating shares subsets in recreating the set[3]. In cutting edge terminology cryptography and security are developing progressively different, cryptography and security are in a general sense in view of issues that are hard to explain. An issue might be troublesome on the grounds that its answer

requires some mystery learning, for example, unscrambling a scrambled message or marking some computerized record [4].

Cryptographic frameworks are for the most part characterized along three autonomous measurements:

- Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged[1]. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition [2].
- The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption [4].
- The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block [4]. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

II EXISTING SYSTEM

The current calculation for encryption mainly depends on the keys, that have been created with in the message that are not necessary to be characterized from the client side, while if we take the past calculation then underlying key should be characterized by the client unequivocally. After the completion of encryption, for the purpose of unscrambling the other side of recipients the key will be exchanged [5]. In this manner key is exchanged on the recipient's side by including the encoded frame for the message.. The other part is performed by irregular generation of the numbers to upgrade security. Further calculation utilizes rail-fence method and its substitution, yet the choice between two encryption strategies which to connect first will be decided by arbitrary number. The utilization of substitution encryption depends on the first message length. After performing both calculations that leads to connected, every character will be applied by NOT door. By chance if message length is even, we will include the key at the end and for the documentation utilized on irregular number to be set towards message starting in terms of bytes otherwise the documentation should be put away toward the last end and start initiation with the key [5]. The documentation will be zero for arbitrary number on the off chance that it is even and one in the event that it will be odd. For utilizing the word with five LSB the key will be placed away in a byte. The system will transmit the last message.

By unscrambling calculation at the flip side would isolate not only key but also documentation utilized in case of arbitrary number with the figure message by inspecting length. When the isolation happens, the content in the figure is going to experience operation NOT and unscrambling rounds along these lines will be connected, on the premise of arbitrary number documentation. In the event that irregular number documentation happened to be zero, then rail fence method to be connected first then afterward substitution, otherwise the other way around

2.1 Short comings of existing method

- As it is easy to understand and implement, so it is also easy to evaluate key for the third.
- Efficient Key Generation is not possible all the time with the Transposition techniques.
- Doesn't provide high security as required.
- Brute force attack for Rail Fence is easy
- Uses Basic and easy Encryption schemes.
- Not a Formula based.

III PROPOSED METHOD

In the proposed method, it is hard to evaluate the key for the third party since it generates multiple keys. In the proposed method no algorithm for separating the key is used as text itself entrenched with the key. So, that it provides more security. Here it uses some logical operations for the encryption as well as for decryption. Encryption and decryption is performed in three rounds. Transposition techniques are used to arrange the intermediate cipher text into final cipher text.

3.1 General Procedure

Proposed method processed in two rounds of encryption as follows. Initially it reads the file as input and converts it into equivalent ASCII values. Then, equivalent binary values are calculated for the corresponding ASCII values. From the calculated binary values perform Circular shift then we can obtain the Key1. Now we are again performing XNOR operation on value obtained Key1 and ASCII values of plain text then we can get Intermediate text-1 as that we have to take the average values to that values obtained in round 1. We are performing Ceaser cipher with formula C= (P+K) MOD256. This is said to be as Round 2 in this round we have to generate NOT to the resultant values in previous step to get Final cipher text we have to perform Cantor Pairing Function.

Round 1:

In the first round of encryption, we are taking ASCII values to plaintext and taking average value and again perform circular shifting to get Key1.Logical XNOR operation is performed to the Key1 and the ASCII values of plain text. After obtaing values make average value.

Round 2:

In the second round of encryption, Ceaser cipher is performed for Round 1 result by making use of C = (P+K)MOD 256 so that we can get values for each character and perform NOT to that values to get appropriate values.

Round 3:

Now Cantor pairing function is performed to get the result and the result is cipher text[6]. We can get Cipher text 1 and Cipher text 2. Cipher text that is obtained from the Cantor pairing is double to the plain text.

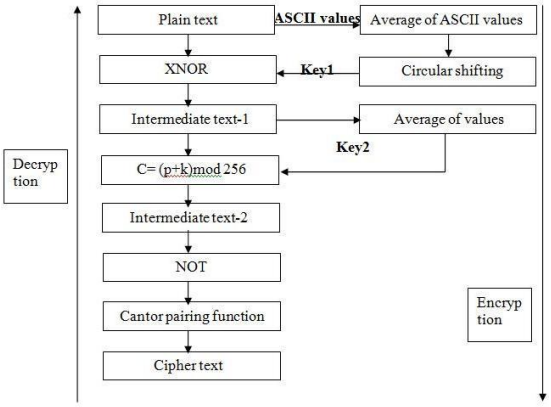
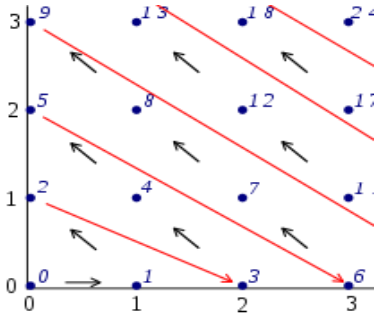


Fig 3.1 General working procedure of proposed system

Cantor pairing: In this proposed calculation proposed a cantor matching capacity keys era is absolutely powerful in light of different variables which leftovers for plain content and content length, the content length is isolated by values of ASCII[6]. The encryption yield is absolutely exist in the numbers configuration and will be in the twofold content of plain for the span. For the part of encryption the blending capacity will be utilized. This is a procedure for exceptionally encoding two numbers which are common into a solitary regular number [5]. For the process of encryption paring capacity will be utilized and also de-pairing capacity will be utilized as a part of decoding calculation

Cantor pairing function



Each pair of natural numbers is assigned by Cantor pairing function [6].

The **Cantor pairing function** is nothing but a pairing function

$$\pi : N \times N \to N$$

defined by;

$$\pi(k_1, k_2) := \frac{1}{2}(k_1 + k_2)(k_1 + k_2 + 1) + k_2 \qquad (1)$$

The pairing function[1] is;

P(a,b)= ((a+b)2+3a+b)/2 = N (2)

Where a= Text, b= Key, N = Integer value;

a = N - (R*(R+1)/2) (3)

b = ((R*(R+3))/2)-N (4)

From the view of Logical operations like NOT and XOR bitwise and mathematical operations will be utilized as a part of this calculation to make dissemination and perplexity. Alongside these paired transformations and decimal changes are additionally utilized. Notwithstanding these blending capacity is utilized as a part of encryption calculation and de-matching capacity is utilized as a part of unscrambling.

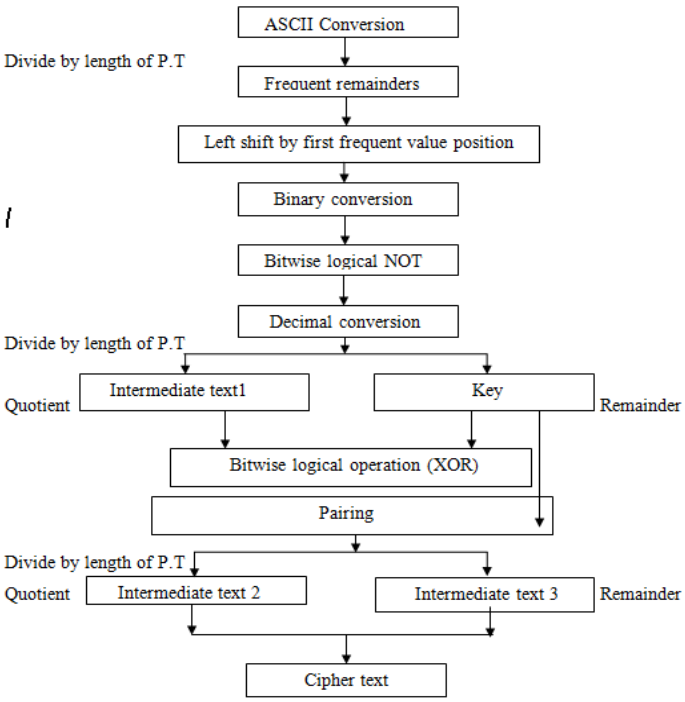


Fig 3.2 Decryption is reverse to this.

3.2 Algorithm for Encryption

Step1: BEGIN.

Step2: Reading the plain text.

Step3: Convert plaintext to equivalent ASCII values and take average to it.

Step4: Perform Left Circular shift by the length of plain text, and make Logical XNOR to that.

Step5: We can get Intermediate text-1 again taking average to that to get Key2.

Step6: Perform Caesar Cipher to that to get Intermediate text-2 and perform NOT operation to it.

Step7: Apply Cantor pairing function to that values obtain in the previous steps.

Step8: Here we can get Cipher text-1 and Cipher text -2.

Example: Plain text is" won "

Step1: Taking ASCII values of input

word "won". (w=119,o=111,n=110).

Step2: By calculating average values of all ASCII (Key) is

(119+111+110)/3=113

Step3: 113=01110001.

perform left circular shift by the length of plain text(3)

times. and the result is " 10001011 " ,which is key 1.

Step4: XNOR operation between "w" and key1

10001011(key1)

01110111 (w)

00000011(03) ⟶ R1

XNOR operation between "o" and key1

10001011(key1)

01101111 (0)

00011011(27) ⟶ R1

XNOR operation between "n" and key1

10001011(key1)

01101110(n)

00011010(26) ⟶ R1

Step5: average of R1 : (03+26+27) /3 =18.(key 2)

Step6: C=(R1+key2) mod 256.

w =>(03+18)mod 256= (21)mod 256 = 21.
o =>(27+18)mod 256= (45)mod 256 = 45. } R 2
n =>(26+18)mod 256= (44)mod 256 = 44.

Step7: NOT operation of R2

w =>NOT(21) =>NOT(00010101) =>(11101010) = 234.

o => NOT(45) =>NOT(00101101) =>(11010010) = 210.

n =>NOT(44) =>NOT(00101100) =>(11010011) = 211

Step8: After applying Cantor pairing function

Cipher text1 is 40 35 09

Cipher text2 is 00 02 01

Decryption in Proposed System

Decryption is performed in rounds. Here cipher text will be given as input and the output will be the plain text.. Normally in case of decryption, with no user interaction it can only decrypt the data with the help of key only.

Round 1

In the first round of decryption it takes the input as the cipher text. Here the cipher text will be subjected to the De-Pairing function that means here the intermediate cipher text is obtained as like the result generated after second round of encryption[6]. Performing NOT to the values obtained from De-pairing function to get the intermediate cipher text.

Round 2

Ceaser function is performed on the intermediate cipher text in this second round of decryption[5]. Here the ASCII values for the intermediate cipher text are calculated. And the obtained result will be performed with XNOR Logical operation and those ASCII values are converted into binary values. Thus the resultant Plain text is obtained in this decryption.

3.3 Algorithm for decryption

Step1: Begin.

Step2: Read the resultant cipher text as the input file.

Step3: Calculate the Cantor De-Pairing function.

Step4: Performing NOT to the values from previous step.

Step5: Apply P=(C-K) mod 256 to the Intermediate text-1 in above step. Where c is Cipher text and k is Key2 taken from encryption to get Intermediate text-2

Step6: Calculate XNOR to the values of previous steps with Key1 taken from encryption.

Step 7: Thus the obtained result is the plain text.

Step 8: Stop.

Example:

Step1**:**

DEPAIRING FUNCTION:

40 35 09 00 02 01

Length(L):6.

First (L/2) values cipher text 1: 40 35 09.

Second (L/2) values cipher text 2: 00 02 01.

Intermediate text ((L/2)* cipher text 1)+cipher text 2) :

((3*40)+0)	((3*35)+02)	((3*09)+01)
120	107	28.

Step2**:** The De-pairing function is

R=(sqrt(8N+1)-1)/2

Where a=text ,b=key ,N=integer value

a=N-(R*(R+1)/2); (N value from pairing function)

b= ((R*(R+3))/2)-N; (R value from de_ pairing)

text: 15 12 07

Key is : 00 02 00

Step3: Perform NOT to text3 we can get text4: 210 211 234

Remainders of decimal (Divide by (L/2)): 0 1 0

Frequent remainder positions compared with first: 0

Select last remainder position: 2

Left rotate text-4 by 2 times

After rotation the result is: 234 210 211

Perform not operation:

234(11101010) =>00010101(21)

210(11010010) =>00101101(45)

211(11010011) =>00101100(44)

Intermediate text(C): 21 45 44

Step4: Perform mod operation

P=(C-Key2) mod 256

w=> (21-18) mod 256=(03)mod 256=03

o=> (45-18) mod 256=(27)mod 256=27

n=> (44-18) mod 256=(26)mod 256=26

Step5: XNOR operation between above values and Key1

XNOR (139, 03) =01110111=119(w)

XNOR (139, 27) =01101111=111(o)

XNOR (139, 26) =01101110=110(n)

Equivalent plain text is: "won"

IV CONCLUSION

Organize security is a critical area which is progressively making up a lot considerations as and when the web grows. The essential security innovation is decided by examining the web conventions and security dangers. The enhancement in the notion of the security innovation is based on programming, further multiple regular equipment gadgets are utilized regularly. The system security advancement at present is not exceptionally amazing. At last proposed framework reasons that key created by this calculation is likewise symmetric key. There is no requirement for independent key era calculation as key is produced from the plain content or figure message by the process of encryption or decoding calculation. Blending capacity utilized here is an unmistakable capacity that can't be found as a rule calculation which is one of the qualities of this proposed calculation. The set of applications is going to drive the network security than anything else. In future the proposed method may be extended to 512 rotations instead of 256 bits rotation. It will be useful in generating cipher text randomly and effectively that more number of special characters are added. In future it provides more complex and confusing for cryptanalysis.

REFERENCES

[1] S. William, "Cryptography and Network Security: Principles and Practice", 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.

[2] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

[3] Behrouz A, Forouzan, "Cryptography and Network Security", Special Indian Edition, TATA McGraw Hill.

[4] K. Gary, "An Overview of Cryptography", an article available at www.garykessler.net/library/crypto.html

[5] R.Venkateswaram, Dr.V.Sundaram, (2010), "Information Security: Text Encryption and Decryption with Poly Substitution method and combining features of cryptography"

[6] Dr. B Reddaiah "A Study on Pairing Functions for Cryptography", International Journal of Computer Applications (0975-8887), Volume 149 – No.10, September 2016