Research Article Impact Factor: 0.621 ISSN: 2319-507X
Sonali Kulkarni, IJPRET, 2014; Volume 2 (9): 220-224 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CRYPTOGRAPHIC ALGORITHM FOR SECURITY

SONALI PRAMOD KULKARNI

Asst. Professor, Department Of Computer Science, Fergusson College, Pune.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Today most of the people use internet for transferring important messages over the internet which may be of company related or college or self related messages. But for websites through which we transfer money or our important messages to other persons, it is required to maintain our transactions or discussion secure. And for this, we require proper cryptographic algorithm which will maintain security over the internet. So this paper presents the new cryptography algorithm for security.

Keywords: Encryption, Decryption, Plain text, cipher text

Corresponding Author: MS. SONALI PRAMOD KULKARNI

Access Online On:

www.ijpret.com

How to Cite This Article:

Sonali Kulkarni, IJPRET, 2014; Volume 2 (9): 220-224

PAPER-QR CODE

INTRODUCTION

Cryptography is useful when sender and receiver send messages to each other and they want to keep their data secrete. For this, we use four terms:

1) Plain text 2) Cipher text
3) Encryption 4) Decryption

Plain text is our actual data which we want to send and receive. Cipher text is the data which is in non-readable format to get security. In encryption, we convert plain text into cipher text and in decryption; we convert cipher text into plain text. Figure 1 shows Plain text, Cipher text, Encryption, Decryption:

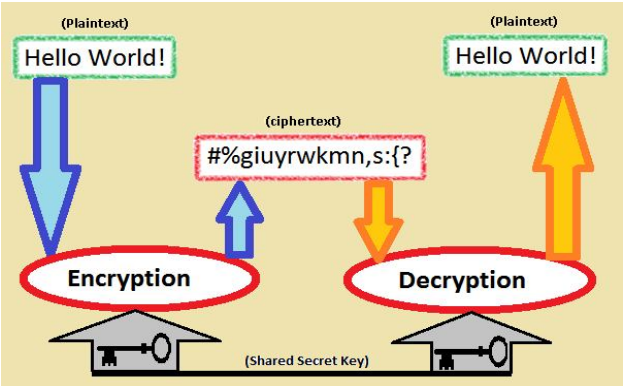

Fig. 1 Image Which Contains Plain Text, Cipher Text, Encryption, Decryption [1]

LITERATURE REVIEW:

Meaning of the cryptography is writing secrete things [2] so that it is hard to crack original data for hackers. We can use either '***transposition technique'*** or '***substitution technique'***.

1) Transposition Technique: In this, we replace one or more characters with other characters.(3) **E.g.**: We can replace z with y etc.

2) Substitution Technique: In this, we rearrange the text. Example: Replace 1st character with 4th, 2nd with 5th, etc.(3) **E.g.**: We can replace 6^{th} character with 1^{st} character etc.

Implementation:

We take "***cryptography is great"*** as a plain text.

Encryption:

Step 1: Draw three circles and each must be divided into 8 equal parts; **Second Circle, First Circle, Third Circle** respectively**.** This is shown in the figure 2:

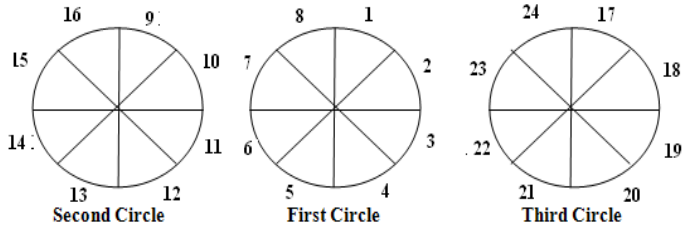

Fig 2 Second Circle, First Circle and Third Circle each of which is divided into 8 equal parts

Step 2: Write the first character into section 1 of second circle, second character of first world into section 2 and so on. If second circle is completed by all the characters then go to the first circle, write down the respected character into section 9[section 9`s character is the character which comes after the 8$^{th}$ section`s character]. Then complete the first circle. After completing the first circle, go to third circle and fill the remaining section of the third circle by writing respective section number if the characters are not present in the words. All the three circles with filled characters and numbers are shown in figure 3:

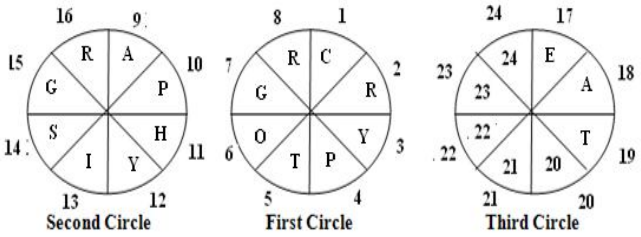

Fig. 3 All the three circles with filled characters and numbers

Step 3: Combine all the characters and that will be our cipher text.

I] A I C T E _ P S R O P _ H G Y G T _ Y R P R _ _
II] 9 13 15 17 21 10 14 2 6 18 22 11 15 3 7 19 23 12 16 4 8 20 24

[I] indicates the cipher text which we want and II] is the section number of the respected circles]

Descryption:

Step 1: Draw three circles and each must be divided into 8 equal parts; **Second Circle, First Circle, Third Circle** respectively**.** This is shown in the figure 4:

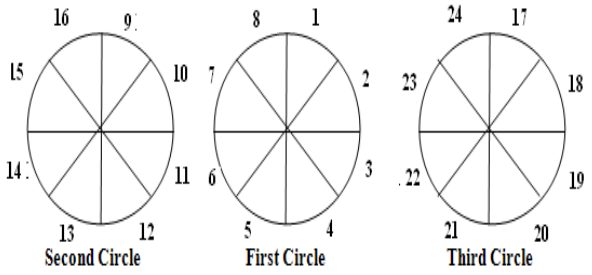

Fig. 4 Second Circle, First Circle and Third Circle each of which is divided into 8 equal parts

Step 2: Put first character of the cipher text in section 9 of the circle two. And second character to the section 13 which is exactly in front of the section 9 of circle two, third character to section 1 and fourth character to section 5, fifth character to section 17, sixth character to section 21,seventh character to section ten, eighth character to section 14 which is exactly opposite to section 10, ninth character to section two and tenth character to section six, eleventh character to section eighteenth, 12th character to section 22 and keep on inserting the characters in the different sections of the circles clockwise till the end of the circle section. All the three circles with filled characters and numbers are shown in figure 5:

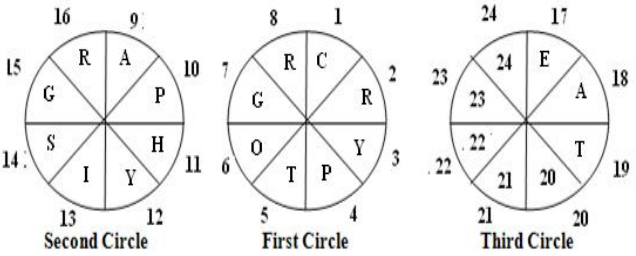

Fig. 5 All the three circles with filled characters and numbers

Step 3: Write down characters from section 1 to section 24 respectively and that will be the plain text which we want.

Thus the plain text obtained is: **CRYPTOGRAPHY IS GREAT**

Note: From word 1 to words 3, draw 3 circles which will be divided into 8 equal parts each. If sections of the circles are remaining blank then put that respected section number over there. If there are more characters in the 1 to 3 words[i.e. more than 24 characters] then only add

fourth circle which should be divided into same 8 equal sections and follow the sequence of the circle as first, second, third, fourth etc for encryption as well as decryption.

CONCLUSION:

By using this algorithm, we will get security since we are putting all the numbers or characters of all the words into different section of the circles and for writing cipher text and plain text, we are putting exactly opposite section`s characters together which will be harder for hacker to hack the cipher text.

REFERENCES:

1. https://www.google.co.in/search?q=cryptography&biw=1024&bih=634&tbm=isch&tbo=u&source=univ&sa=X&ei=ezsXU9joJMWUrgfQ4ICgBA&sqi=2&ved=0CDkQsAQ#facrc=_&imgdii=_&imgrc=zhAeL3bf7dDUM%253A%3Bghih9TsPuuKjAM%3Bhttp%253A%252F%252Fupload.wikimedia.org%252Fwikipedia%252Fcommons%252Ff%252Ff8%252FCrypto.png%3Bhttp%253A%252F%252Fen.wikipedia.org%252Fwiki%252FCryptography%3B603%3B404

2. http://en.wikipedia.org/wiki/Cryptography

3. Atul Kahate, Cryptography and Network Security, ISBN 0-07-049483-5, eBook