INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed Refereed Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.

as well as in Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)]

Registered & Listed at: Index Copernicus Publishers Panel, Poland

Circulated all over the world & Google has verified that scholars of more than 1500 Cities in 141 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

www.ijrcm.org.in

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:** These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

AN ENHANCE SECURITY OF PLAYFAIR CIPHER SUBSTITUTION USING A SIMPLE COLUMNAR TRANSPOSITION TECHNIQUE WITH MULTIPLE ROUNDS (SCTTMR)

GAURAV SHRIVASTAVA
ASST. PROFESSOR
DEPARTMENT OF INFORMATION TECHNOLOGY
SHRI VAISHNAV INSTITUTE OF TECHNOLOGY & SCIENCE
INDORE

MANOJ DHAWAN
ASST. PROFESSOR
DEPARTMENT OF INFORMATION TECHNOLOGY
SHRI VAISHNAV INSTITUTE OF TECHNOLOGY & SCIENCE
INDORE

MANOJ CHOUHAN
ASST. PROFESSOR
DEPARTMENT OF INFORMATION TECHNOLOGY
SHRI VAISHNAV INSTITUTE OF TECHNOLOGY & SCIENCE
INDORE

ABSTRACT

In this paper, we have made use of a traditional Playfair cipher technique with Simple Columnar Transposition Technique with Multiple Rounds (SCTTMR). After applying SCTTMR we got the actual cipher. Our main focus is on the Playfair Cipher, its advantages and disadvantages. Finally, we have proposed methods to enhance the Playfair cipher for more secure and efficient cryptography which provide difficulty in identifying individual diagram.

KEYWORDS

Playfair Cipher, Simple Columnar Transposition Technique, SCTTMR, Substitution Cipher.

INTRODUCTION

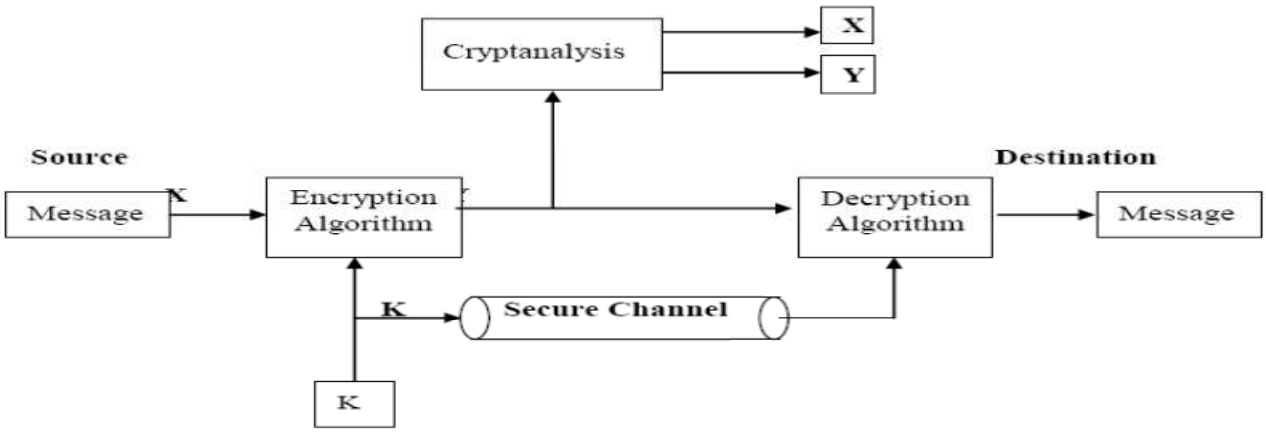
From the beginning of human society, people have been very much concerned with the privacy of their communications. In contemporary societies, the growing use of computer has made the security of digital files of outmost concern against those users with malevolent intentions, especially on the internet. To protect the digital files either in the computer or in the transmission [2],

Cryptography is the science which deals with all the means and methods for converting an intelligible message into an unintelligible or secret form and for reconverting the secret form into the intelligible message by a direct reversal of the steps used in the original process [1]. Even though encryption is very powerful among these two, the cryptanalysts are very intelligent and they were working day and night to break the ciphers. To make a stronger cipher it is recommended that to use: More stronger and complicated encryption algorithms with more number of rounds, Keys with more number of bits (Longer keys), secure transmission of keys [3].

CRYPTOGRAPHY SCIENCE

The word is derived from the Greek crypto's, meaning hidden. Cryptography is a science of devising methods that allow information to be send in a secure from in such a way that the only person to able retrieve this information is the intended recipient. Encryption is based on algorithms that scramble information (Plaintext or Clear Text) into unreadable (Cipher Text) form. Decryption is the process of restoring the scrambled information to its original form. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. Cryptographic systems are used to provide privacy and authentication in computer and communication systems. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. [9]

FIGURE 1: CRYPTOGRAPHIC SYSTEM



All Cryptographic algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, and group of bits or letters) is mapped into another element and in transposition, the elements of the plaintext have simply been re-arranged in different order; their position with relation to each other have been changed. [4]

CLASSIC CRYPTOGRAPHY

The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. More literacy, or literate opponents, required actual cryptography. The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g., 'hello world' becomes 'ehlol owrdl' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet). [9]

- **Substitution Technique**

In cryptography, a substitution cipher is a method of encryption by which units of plaintext are replaced with cipher text according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

There are a number of different types of substitution cipher available like Caesar Cipher, Mono-alphabetic Cipher, Homophonic Substitution Cipher, Polygram Substitution Cipher, Polyalphabetic Substitution Cipher, Playfair Cipher and Hill Cipher. [9]

- **Transposition Technique**

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

There are a number of different types of Transposition cipher available like Rail Fence Cipher, Simple Columnar Transposition, Vernam Cipher, Double transposition, Myszkowski Transposition, Disrupted Transposition. [9]

PLAYFAIR CIPHER

The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 600 possible digraphs rather than the 26 possible monographs. The frequency analysis of digraphs is possible, but considerably more difficult – and it generally requires a much larger cipher text in order to be useful. [8]

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.

To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.[8]

To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "Hello World" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append a "Z" to complete the final digraph. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same, add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively.
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively.
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair. [8]

To decrypt, use the INVERSE (opposite) of the last 3 rules, and the 1st as-is (dropping any extra "X"s (or "Q"s) that don't make sense in the final message when finished).

Example:-

Key is "Playfair example" the table becomes

TABLE 1

P	L	A	Y	F
I/J	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Message is "Hide the gold in the tree stump":

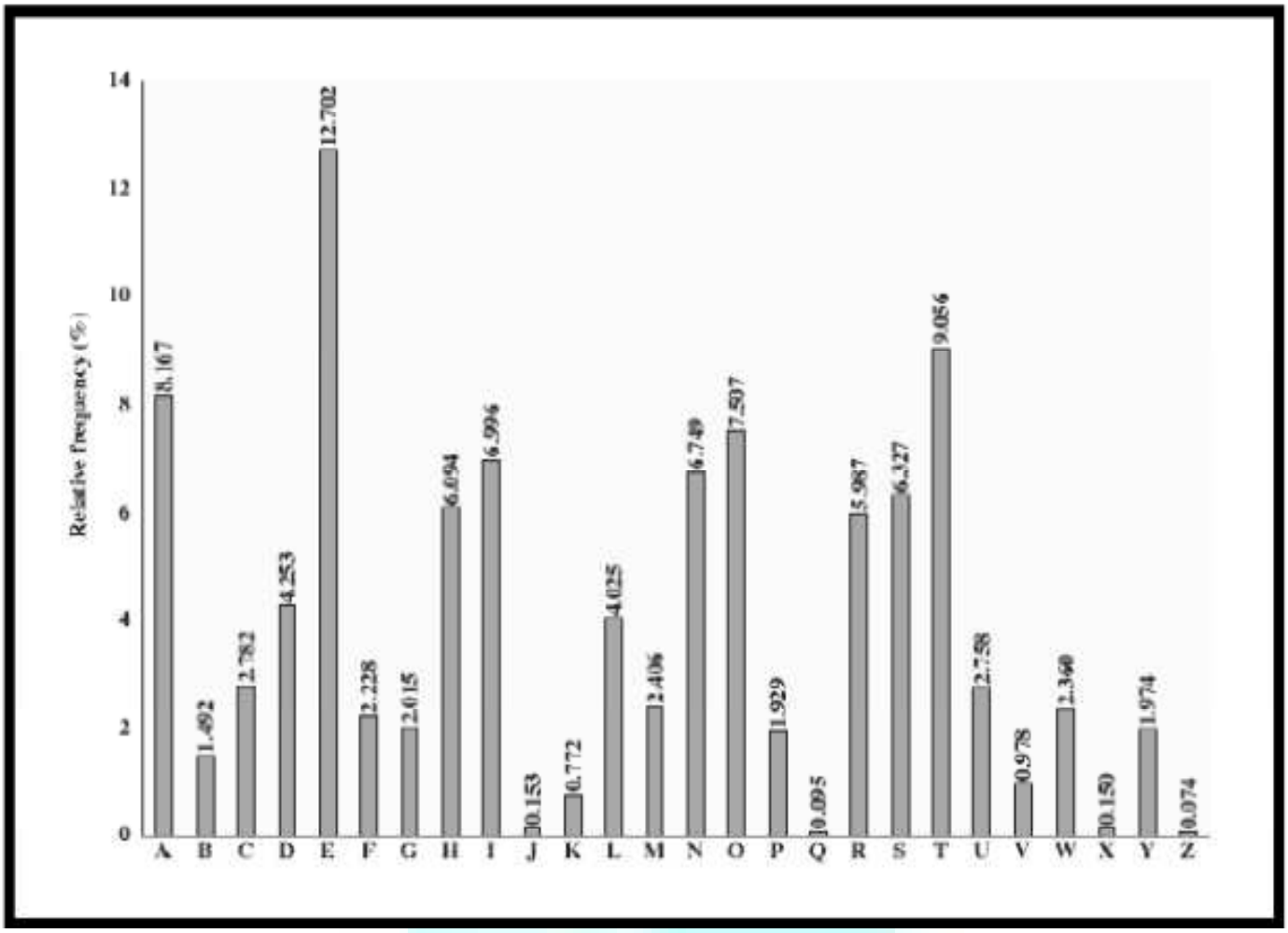
To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, becomes “HI DE TH EG OL DI NT HE TR EX ES TU MP”

Thus the Message (Plain Text) "Hide the gold in the tree stump" becomes "BMNDZBXDKYBEJVDMUIXMMNUVIF".

PRAPOSED PLAYFAIR CIPHER

From the Figure-2, we can notice that, the frequency of the letter I is 6.996 and J is 0.153. These are widely used letters in normal text and considered as a single letter in the Playfair Table-I. It may leads to the confusion at the receiving side whether to use I / J for decryption. [4]

FIGURE 2: RELATIVE FREQUENCY OF LETTERS IN ENGLISH TEXT



To reduce the ambiguity at the receiving end, it is better to combine the less frequency letters as a one letter in the Table-I rather than using I/J as single letter. So, that the less frequency letters appears very rare in the text and hence we can reduce the confusion level while decrypting at the receiving end. For this we recommend to combine Q (0.095) and Z (0.074) as a single letter in the Playfair Table 2.

For constructing the Table-2 we rearranged the 26 letters in 5X5 matrix by considering the frequency of letters from the Figure-2. Use the keyword and fill the keyword characters from left to right and top to bottom in the matrix, then fill the least frequency letters Q/Z count as one letter, after that fill the remainder of the matrix with the remaining letters in alphabetic order. [4]

TABLE 2

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q/Z	R	S	T
U	V	W	X	Y

In above metrics we apply a Simple Columnar Transposition Technique with Multiple Rounds.

HOW TO APPLY MULTIPLE ROUNDS

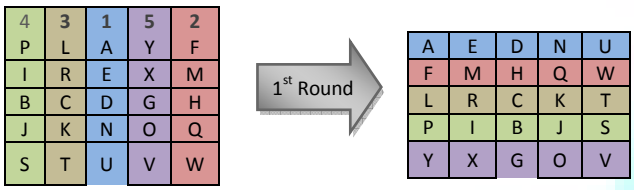
1. Using the keyword we arrange the keyword character from left to right and fill the 5X5 matrices with remaining character.
2. We mark the first row of matrices with 1, 2,3,4,5 according the dictionary order.
3. Rearranged the first marked column in first row which makes the first round.
4. In next round we mark the second row according to step 2.
5. Then fallow the steps 2 to 4.
6. Follow the steps 2 to 5 for 5 round.

Example

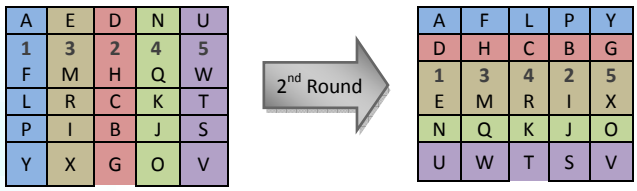
Key is "Playfair example" the table becomes

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
J	K	N	O	Q/Z
S	T	U	V	W

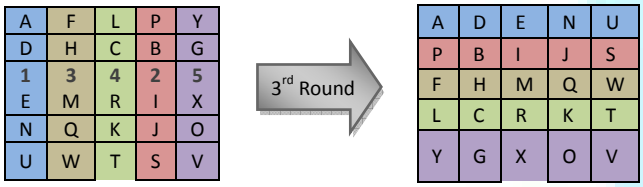
1st Round



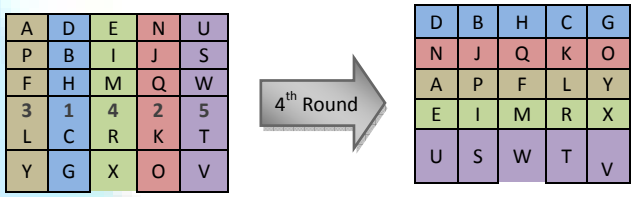
2nd Round



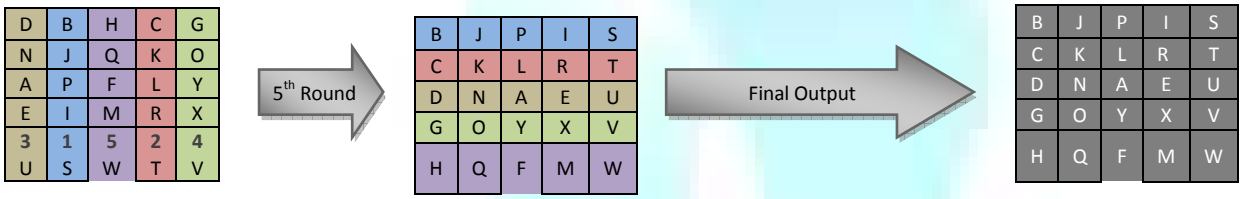
3rd Round



4th Round



5th Round



Message is "Hide the gold in the tree stump":
In this Message (Plain Text) we apply all rules of existing Playfair cipher in section 4 of this paper.
"HI DE TH EG OL DI NT HE TR EX ES TU MP" becomes
"MBNUCWDXYKEBUKMDCTXMUIUVFI".

RESULT

With our enhanced Playfair Cipher Technique with SCTTMR is observed that, it can be used for the plaintext with Multiple Rounds which makes the encryption complex and difficult to identify individual diagram. It is also noticed that, by combining less frequency character 'Q/Z' instead of 'I/J' the ambiguity at receiving end will be reduced.

ADVANTAGE OF PRAPOSED PLAYFAIR TECHNIQUE

- Identification of individual diagrams is difficult.
- Frequency analysis difficult.

CONCLUSION

In this paper we have combine two different approach Substitution and Transposition Technique including Simple Columnar Transposition Technique with Multiple Rounds (SCTTMR). To solve the de merits in Playfair we have proposed and explained methods with examples. For this, we provide multiple rounds which make the complex encryption. Finally we named it as: '**An Enhance Security of Playfair Cipher Substitution Using a Simple Columnar Transposition Technique with Multiple Rounds (SCTTMR)** '. The present version of the play fair technique will consider only text in English for conversion; we can also extend it to numbers and symbols for wide range of use.

REFRENCES

1. Beker. H and Piper. F, "Communications Survey: a survey of Cryptography", IEEE Proc. A, 357-376, 1982.
2. G. J. Simmons, "Symmetric and asymmetric encryption", ACM Compute Surveys, 305-330, 11, 1979
3. "Data Security", ACM Compute Surveys, 227-250, 11, 1979.
4. Ravindra Babu Kallam, "An Improved Playfair Cipher Cryptographic Substitution Algorithm",Volume 2, No. 1, Jan-Feb 2011 IJARCS, ISSN No. 0976-5697
5. Atul Kahate, Cryptography and Network Security, Second Edition, the McGraw-Hill Companies.
6. William Stallings, Cryptography and Network Security, Prentice Hall of India Private Limited, New Delhi.
7. http://reusablesec.blogspot.in/2009/05/character-frequency-analysis-info.html
8. http://en.wikipedia.org/wiki/Playfair_cipher
9. http://en.wikipedia.org/wiki/Cryptography

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, IT and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail i.e. **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals