INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) 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 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 1667 Cities in 145 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

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	**EFFICIENCY AND PERFORMANCE OF e-LEARNING PROJECTS IN INDIA** *SANGITA RAWAL, DR. SEEMA SHARMA & DR. U. S. PANDEY*	1
2.	**AN ADAPTIVE DECISION SUPPORT SYSTEM FOR PRODUCTION PLANNING: A CASE OF CD REPLICATOR** *SIMA SEDIGHADELI & REZA KACHOUIE*	5
3.	**CONSTRUCT THE TOURISM INTENTION MODEL OF CHINA TRAVELERS IN TAIWAN** *WEN-GOANG, YANG, CHIN-HSIANG, TSAI, JUI-YING HUNG, SU-SHIANG, LEE & HUI-HUI, LEE*	9
4.	**FINANCIAL PLANNING CHALLENGES AFFECTING IMPLEMENTATION OF THE ECONOMIC STIMULUS PROGRAMME IN EMBU COUNTY, KENYA** *PAUL NJOROGE THIGA, JUSTO MASINDE SIMIYU, ADOLPHUS WAGALA, NEBAT GALO MUGENDA & LEWIS KINYUA KATHUNI*	15
5.	**IMPACT OF ELECTRONIC COMMERCE PRACTICES ON CUSTOMER E-LOYALTY: A CASE STUDY OF PAKISTAN** *TAUSIF M. & RIAZ AHMAD*	22
6.	**SOCIAL NETWORKING IN VIRTUAL COMMUNITY CENTRES: USES AND PERCEPTION AMONG SELECTED NIGERIAN STUDENTS** *DR. SULEIMAN SALAU & NATHANIEL OGUCHE EMMANUEL*	26
7.	**EXPOSURE TO CLIMATE CHANGE RISKS: CROP INSURANCE** *DR. VENKATESH. J, DR. SEKAR. S, AARTHY.C & BALASUBRAMANIAN. M*	32
8.	**SCENARIO OF ENTERPRISE RESOURCE PLANNING IMPLEMENTATION IN SMALL AND MEDIUM SCALE ENTERPRISES** *DR. G. PANDURANGAN, R. MAGENDIRAN, L.S. SRIDHAR & R. RAJKOKILA*	35
9.	**BRAIN TUMOR SEGMENTATION USING ALGORITHMIC AND NON ALGORITHMIC APPROACH** *K.SELVANAYAKI & DR. P. KALUGASALAM*	39
10.	**EMERGING TRENDS AND OPPORTUNITIES OF GREEN MARKETING AMONG THE CORPORATE WORLD** *DR. MOHAN KUMAR. R, INITHA RINA.R & PREETHA LEENA .R*	45
11.	**DIFFUSION OF INNOVATIONS IN THE COLOUR TELEVISION INDUSTRY: A CASE STUDY OF LG INDIA** *DR. R. SATISH KUMAR, MIHIR DAS & DR. SAMIK SOME*	51
12.	**TOOLS OF CUSTOMER RELATIONSHIP MANAGEMENT – A GENERAL IDEA** *T. JOGA CHARY & CH. KARUNAKER*	56
13.	**LOGISTIC REGRESSION MODEL FOR PREDICTION OF BANKRUPTCY** *ISMAIL B & ASHWINI KUMARI*	58
14.	**INCLUSIVE GROWTH: REALTY OR MYTH IN INDIA** *DR. KALE RACHNA RAMESH*	65
15.	**A PRACTICAL TOKENIZER FOR PART-OF SPEECH TAGGING OF ENGLISH TEXT** *BHAIRAB SARMA & BIPUL SHYAM PURKAYASTHA*	69
16.	**KEY ANTECEDENTS OF FEMALE CONSUMER BUYING BEHAVIOR WITH SPECIAL REFERENCE TO COSMETICS PRODUCT** *DR. RAJAN*	72
17.	**MANAGING HUMAN ENCOUNTERS AT CLASSROOMS - A STUDY WITH SPECIAL REFERENCE TO ENGINEERING PROGRAMME, CHENNAI** *DR. B. PERCY BOSE*	77
18.	**THE IMPACT OF E-BANKING ON PERFORMANCE – A STUDY OF INDIAN NATIONALISED BANKS** *MOHD. SALEEM & MINAKSHI GARG*	80
19.	**UTILIZING FRACTAL STRUCTURES FOR THE INFORMATION ENCRYPTING PROCESS** *UDAI BHAN TRIVEDI & R C BHARTI*	85
20.	**IMPACT OF LIBERALISATION ON PRACTICES OF PUBLIC SECTOR BANKS IN INDIA** *DR. R. K. MOTWANI & SAURABH JAIN*	89
21.	**THE EFFECTIVENESS OF PERFORMANCE APPRAISAL ON ITES INDUSTRY AND ITS OUTCOME** *DR. V. SHANTHI & V. AGALYA*	92
22.	**CUSTOMERS ARE THE KING OF THE MARKET: A PRICING APPROACH BASED ON THEIR OPINION - TARGET COSTING** *SUSANTA KANRAR & DR. ASHISH KUMAR SANA*	97
23.	**WHAT DRIVE BSE AND NSE?** *MOCHI PANKAJKUMAR KANTILAL & DILIP R. VAHONIYA*	101
24.	**A CASE APPROACH TOWARDS VERTICAL INTEGRATION: DEVELOPING BUYER-SELLER RELATIONSHIPS** *SWATI GOYAL, SONU DUA & GURPREET KAUR*	108
25.	**ANALYSIS OF SOURCES OF FRUIT WASTAGES IN COLD STORAGE UNITS IN TAMILNADU** *ARIVAZHAGAN.R & GEETHA.P*	113
26.	**A NOVEL CONTRAST ENHANCEMENT METHOD BY ARBITRARILY SHAPED WAVELET TRANSFORM THROUGH HISTOGRAM EQUALIZATION** *SIBIMOL J*	119
27.	**SCOURGE OF THE INNOCENTS** *A. LINDA PRIMLYN*	124
28.	**BUILDING & TESTING MODEL IN MEASUREMENT OF INTERNAL SERVICE QUALITY IN TANCEM – A GAP ANALYSIS APPROACH** *DR. S. RAJARAM, V. P. SRIRAM & SHENBAGASURIYAN.R*	128
29.	**ORGANIZATIONAL CREATIVITY FOR COMPETITIVE EXCELLENCE** *REKHA K.A*	133
30.	**A STUDY OF STUDENT'S PERCEPTION FOR SELECTION OF ENGINEERING COLLEGE: A FACTOR ANALYSIS APPROACH** *SHWETA PANDIT & ASHIMA JOSHI*	138
	REQUEST FOR FEEDBACK	146

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

UTILIZING FRACTAL STRUCTURES FOR THE INFORMATION ENCRYPTING PROCESS

UDAI BHAN TRIVEDI
ASSOCIATE PROFESSOR
INSTITUTE OF MANAGEMENT STUDIES
DEHRADUN

R C BHARTI
ASST. PROFESSOR
INSTITUTE OF MANAGEMENT STUDIES
DEHRADUN

ABSTRACT

Information security is the process which describes all measures taken to prevent unauthorized use of electronic data, whether this unauthorized use takes the form of destruction, disclosure, modification, or disruption. Information security and Cryptography are interconnected and share the common services of protecting the confidentiality, integrity and availability of the information. In the encryption process, information security uses Cryptography to shift the information into the cipher form which does not allow it to be used by unauthorized personnel. Cryptography is one of the most important fields in computer security. It is a method of transferring private information and data through open network communication, so only the receiver who has the secret key can read the encrypted messages which might be documents, phone conversations, images or other form of data. To implement privacy simply by encrypting the information intended to remain secret can be achieved by using methods of Cryptography. The information must be scrambled, so that other users will not be able to access the actual information. In this paper we propose new public-key primitives based on Mandelbrot and Julia Fractal sets. The Fractal based key exchange protocol is possible because of the intrinsic connection between the Mandelbrot and Julia Fractal sets. In the proposed protocol, Mandelbrot Fractal function takes the chosen private key as the input parameter and generates the corresponding public key. Julia Fractal function is then used to calculate the shared key based on the existing private key and the received public key.

KEYWORDS
fractal structures, information encrypting process.

I. INTRODUCTION

1.1) MANDELBROT SETS

In mathematics the Mandelbrot set, named after Benoit Mandelbrot. The Mandelbrot Fractal (see Figure 1(a)) can be defined as the set of complex values of *c (Parameter Space)* for which the orbit of 0 under iteration of the complex quadratic polynomial equation (1)

$$Z_n = Z_{n-1}^2 + c\ ;\ Z_0 = 0;\ \ c, Z_{n-1} \in C; n \in Z\ .$$ remains bounded.

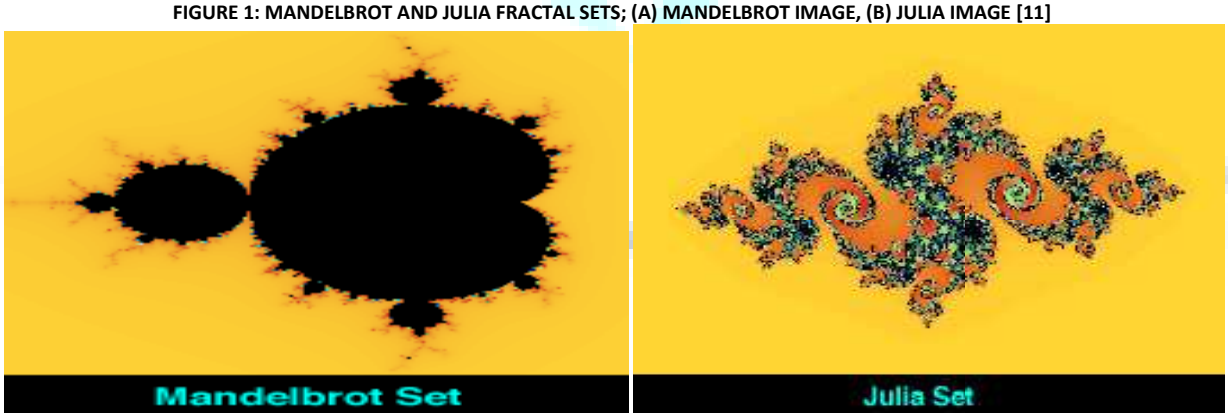
1.2) JULIA SETS

French mathematician Gaston Julia [12] investigated the iteration process of a complex function intensively, and attained the Julia set, Similar to Mandelbrot Fractal set, Julia Fractal set (see Figure 1(b)) is a set of points on a complex plane(state space) defined recursively by Equation 2.

$$Z_n = Z_{n-1}^2 + c\ ;\ \ c, Z_n \in C; n \in Z\ . \qquad (2)$$

The Julia set for parameter is defined as the boundary between those of that remain bounded after repeated iterations and those escape to infinity. The Julia set on the real axis are reflection symmetric, while those with complex parameter show rotation symmetry with an exception to c= (0, 0) see Rani and Kumar [11]. The difference between the Mandelbrot set and the Julia set is that the Mandelbrot set iterates Z^2+c with Z starting at 0 and varying c with every iteration, while Julia set iterates Z^2+c for fixed c and starting with non-zero value of Z [6, 10]. The connection between the Mandelbrot set and the Julia set is that each point c in the Mandelbrot set specifies the geometric structure of the corresponding Julia set [9].

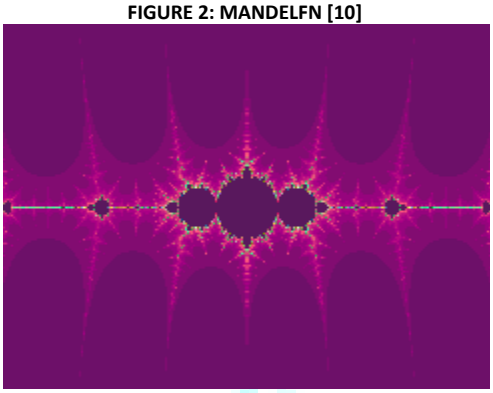
FIGURE 1: MANDELBROT AND JULIA FRACTAL SETS; (A) MANDELBROT IMAGE, (B) JULIA IMAGE [11]



II) MANDELBROT AND JULIA FRACTAL SETS KEY-EXCHANGE PROTOCOL

In this section we will describe the proposed key exchange algorithm in detail. The first step in this protocol is to generate the public key and the private key by using Mandelbrot and Julia functions. The equation used in our proposed protocol is the Mandelbrot function, "*Mandelfn*" (see Equation 4) and Julia function, "*Juliafn*" (see Equation 5). *Mandelfn* is one of the many Mandelbrot functions, and similarly *Juliafn* is a specific form of Julia functions. An image generated from the *Mandelfn* function is shown in Figure 2.

FIGURE 2: MANDELFN [10]



Z (0) = c; c,Z ε C. (3)

Z (n + 1) = c × f (Z (n)); c,Z ε C;n ε Z. (4)

It is easy to generate variation of Fractal images based on *Mandelfn* and *Juliafn* functions. For example, we can substitute the function *f ( )* in Equation 5 and 6 with some known functions such as *sin ( ), cos ( ), exp ( ),* etc., to generate different variation of the functions. However, the generated values from *Mandelfn* must always reside within the Mandelbrot set, and similarly, the values generated by the *Juliafn* must reside within the Julia set [10].

Z (n + 1) = c* f (z (n)) (5)

Z (n + 1) = c × f(Z (n)) ; Z,c ε C; n ε Z. (6)

As shown by Figure 3, Fractal key exchange protocol involves two parties, Alice and Bob. Alice must generate the public key based on her private key as describe earlier. The generated public key is then send to Bob. Bob on the other hand will do the same and send his public key to Alice. To produce the public key, we use Mandelbrot function, *Mandelfn*. For Alice, the generated public key is $Z_n e$, as describes by Equation 7 .

$$Z_n e = Z_{n-1} \times c^2 \times e; Z,c,e \in \mathbb{C}; n \in Z. \quad (7)$$

Similarly for Bob, the generated public key, $Z_k d$, is calculated by using *Madelfn* equation as shown by Equation 8.

$$Z_k d = Z_{k-1} \times c^2 \times d; Z,c,d \in \mathbb{C}; k \in Z. \quad (8)$$

Note that, it is impossible to find the private values from the published public keys, since the iteration, *n*, and the variation constant *e*, are unknown to the public. Hence, we can identify that the hard problem for the proposed Fractal key exchange is through its key selection. This is true since the complex value produces by *Mandelfn* depends on the number of iterations, *n*, as well as the variation constant, *e*, which makes the *Mandelfn* values jump path chaotically. This will prevent attack on the private values, given that *e* is being represented appropriately. We are suggesting *e* to be represented by a 128-bit value which should give 2128 possibilities for every values of *n* that are being brute force. After exchanging the public keys and executing the *Juliafn* function, both Alice and Bob will arrived at the same secret value, $(Z_n e)_k d = (Z_k d)_n e$. Both $(Z_n e)_k d$ and $(Z_k d)_n e$ are equals [1], based on a known Fractal property as shown by Equation 9.

$$c^{n-x} \times (Zkd)_n e = c^{k-x} \times (Z_n e)_k d; \quad (9)$$

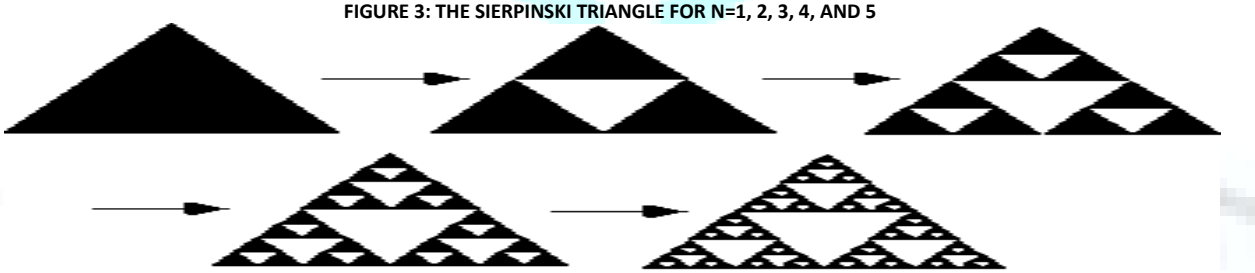
$$Z,c,e,d \in \mathbb{C}; n,x,k \in Z.$$

III) THE SIERPINSKI TRIANGLE FOR ENCRYPTION PURPOSE

The Sierpinski triangle **S** may also be constructed using a deterministic rather than a random algorithm. To see this, we begin with any triangle. Then we use the midpoints of each side as the vertices of a new triangle, which we then remove from the original. This leaves us with three triangles, each of which has area exactly one-fourth of the original area. Also, each remaining triangle is similar to the original.

Now we continue (or iterate) this process. From each remaining triangle we remove the "middle" leaving behind three smaller triangles each of which has dimensions one-half of those of the parent triangle (and one-fourth of the original triangle). Clearly, 9 triangles remain at this stage. At the next iteration, 27 small triangles, then 81, and, at the Nth stage, 3^N small triangles remain. (See Figure 3.)

FIGURE 3: THE SIERPINSKI TRIANGLE FOR N=1, 2, 3, 4, AND 5



The algorithm of generation of Sierpinski Triangle

Void SierTriangle(an equilateral triangle)

If (the triangle is too small)

Stop.

Else

Connect the mid point of the sides with line segments. Color the middle triangle with different color.

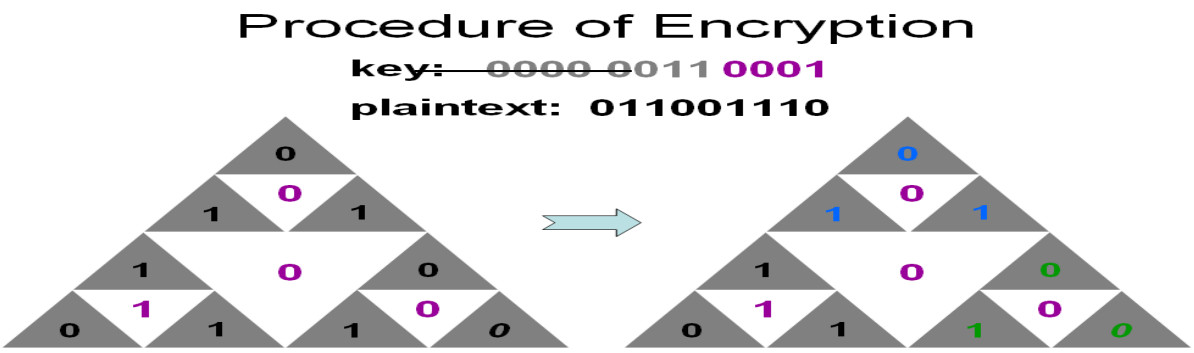
SierTriangle(top triangle)

SierTriangle(bottom left triangle)

SierTriangle(bottom right triangle) //**Figure 4: Algorithm to generate Sierpinski Triangle**

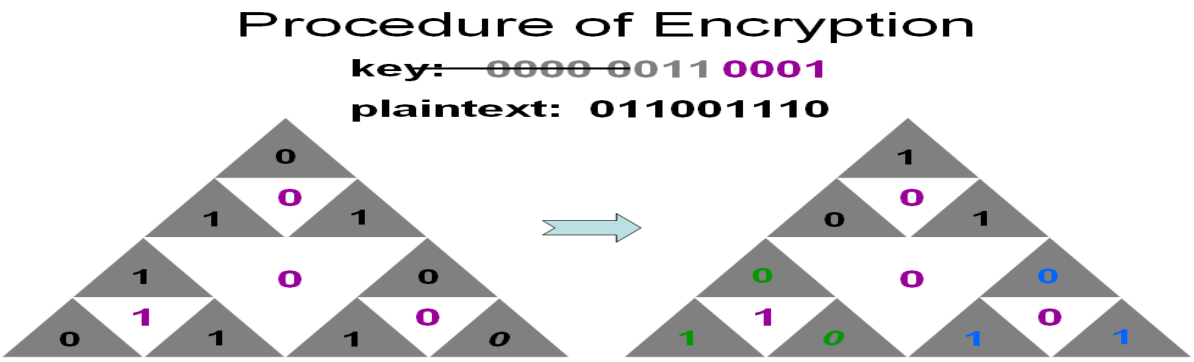
The figure 5 shows I step of encryption by using Sierpinski Triangle. To show the process let us take key as 0001 and plaintext 011001110. The dimension of Sierpinski Triangle should match the key size. The key should arrange in white portion of triangle in CENTER, TOP, LEFT and RIGHT order. The plain text should be arranged in order of generation of Sierpinski Triangle by algorithm shown in figure 4(in black portion triangle) i.e. SierTriangle (top triangle), SierTriangle (bottom left triangle), and SierTriangle (bottom right triangle). The order of arrangement of plaintext with in sub triangle should be TOP, LEFT and RIGHT [7].

FIGURE 5



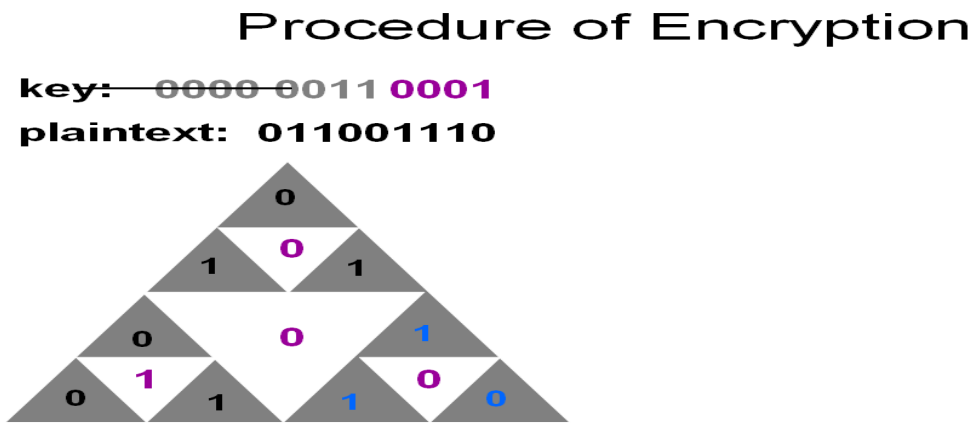
In the II step plaintext content of LEFT triangle should be replace by respective content of TOP triangle, plaintext content of RIGHT triangle should be replace by respective content of LEFT triangle , plaintext content of TOP triangle should be replace by respective content of RIGHT triangle.
Figure 6 shows the value of Sierpinski Triangle after the second step.

FIGURE 6



In the step III The content of TOP, LEFT and RIGHT triangle should rotate by one position in clock wise direction if the corresponding member of key field is 0 (White triangle element) else content of TOP, LEFT and RIGHT triangle should rotate by two position in clock wise direction if the corresponding member of key field is 1 (White triangle element).

FIGURE 6



In the step IV read the content in TOP, LEFT, and RIGHT order to get the Cipher text.
Plain text **011001110** → **cipher text** **011101010**

IV) CONCLUSION

This paper has focus on the how the Mandelbrot and Julia sets can be utilize for the key exchange procedure between sender and receiver. The Fractal based key exchange protocol is made possible because of the intrinsic connection between the Mandelbrot and Julia Fractal sets.
The second half of the paper focus on how, Sierpinski Triangle Fractals can be used for converting Plaintext into cipher text. So, together these two concepts can facilitate the key exchange as well as message encryption.

V) REFERENCES

[1] PhD Thesis on A New Approach To Public-Key Cryptosystem Based On Mandelbrot And Julia Fractal Sets By Mohammad Ahmad A. Alia University Sains Malaysia 2008.

[2] W. Stallings, "Cryptography and Network Security Principles and Practices,"*Pearson Education*, 3rd edition.
[3] Gilbert Helmberg "Getting Acquainted with Fractals"
[4] Mohammad Ahmad Alia and Azman Bin Samsudin, "New Key Exchange Protocol Based on Mandelbrot and Julia Fractal Sets", International Journal of Computer Science and Network Security, Vol. 7, No. 2, February 2007
[5].Douady A., "Julia Sets and the Mandelbrot Set", In the Beauty of Fractals: Images of Complex Dynamical Systems (Ed. H.-O. Peitgen and D. H. Richter). Berlin: Springer- Verlag, pp. 161, 1986.
[6] P. Bourke, "An Introduction to Fractals, "*http://local.wasp.uwa.edu.au/~pbourke/fractals/fracintro/*, May 1991
[7] PENG Hai, GUO Qing-ping, Computer Processing & Distributing Laboratory, Wuhan University of Technology **"**A FRACTAL ENCRYPTION ALGORITHM"
[8] MANDELBROT, B. B., Fractals nad chaos: the Mandelbrot set and beyond. New York: Springer, 2004. 308 s. ISBN 0-387-20158-0.
[9] M. C. Taylor, J. Louvet, "Sci.fractals FAQ," ComputingServices Mount Allison University Sackville, Canada, 1998.
[10] N. Giffin, "Fractint," *TRIUMF project at the University of British Columbia Campus in Vancouver B.C. Canada***,** 2006.
[11] Rani, M.; Kumar, V.: Superior Julia set, J Korea Soc Math Edu Series D: Res Math Edu 2004; 8(4), 261-277.
[12] Julia, G.: Sur 1' iteration des functions rationnelles, J Math Pure Appl., 1918; 8, 47-245

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