A Trusted Model for Securing Shared Resources using Quaternionic Farey Fractions

V.Gayathri[1], Dr.Antony Selvadoss Thanamani[2]

[1]Research Scholar, Vinayaka Mission University, Salem, [2]Reader, NGM College, Pollachi

ABSTRACT:

A data is subjected to variety of attacks. Some attacks are passive in nature in that information is only monitored. Other attacks are active and information is altered with intent to corrupt or destroy the data or the network itself. In the absence of security schemes, both public and private networks are susceptible to unauthorized monitoring and access and can result in system downtime and public exposure to confidential information. At the same time theoretical development in information theory and computer science show promise of providing provably secure cryptosystem. In this context, the objective of this paper is to analyze and implement highly secure cryptography scheme using the properties of quaternion Farey fractions. A cryptography model that can provide high level of confusion and thereby create more diffusion (desirable effect) is proposed in this paper. Use of quaternions has been reported in computer graphics, control theory and signal processing. For example, spacecraft attitude control systems are reported to be commanded in terms of quaternion. The techniques proposed in this paper can help in increasing the accuracy and completeness of network topology discovery and can leverage existing protocol and hardware features, and also can be implemented easily. ***Key words:** Number theory, Computer network Security, Cryptography, resource management*

1. INTRODUCTION

A network is a collection of shared resources and as a result, resource exhaustion can occur due to inefficiently scaling systems, selfish [1,3] resource consumption and malicious attack. Basic services of information security include verification, preserving data integrity, providing non-repudiation and ensuring secrecy. Similarly, integrity threat includes Interception of data, Modification of message, Replay of message, Masquerading and Repudiation. In this context, cryptography can be used to provide confidentiality using encryption methods and can also provide data integrity, authentication and non-repudiation. The purpose of this paper is to deploy number systems [2,3] based cryptography schemes for secure sharing of network resources. The three distinct notions of security models namely cooperative, selfish and malicious users are uniformly taken care in this work. By using the proposed encryption models, it is possible to provide a defense against network attacks and protect the contents of IP packets.

2. QUATERNIONS AND FAREY FRACTIONS

2.1 QUATERNIONS

The quaternion number system was discovered by Hamilton. Quaternions form an extension in the field of complex numbers having the property that the commutative law fails for multiplication, despite the fact that every non-zero element has a multiplicative inverse. Quaternions are expressions of the form a+bi+cj+dk where a, b, c and d are ordinary real numbers. Quaternions have developed a wide-spread use in computer graphics and robotics research because they can be used to control rotations in three dimensional spaces. The order in which quaternions are multiplied is important. The independent co-efficient of the super complex number that has a free rotation in a three dimensional space is taken as the parameter.

2.2 FAREY FRACTIONS

Farey sequences are named after the British geologist John Farey, Sr. Farey conjectured that each term in a Farey sequence[5] is the mediant of its neighbors. The Farey fraction sequence of order i, F(i) consists of all fractions with values between 0 and 1, whose denominators does not exceed i, expressed in lowest terms and arranged in order of increasing magnitude. For example, F(6) is written as,

$$\frac{0}{6},\frac{1}{6},\frac{1}{5},\frac{1}{4},\frac{1}{3},\frac{2}{5},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},\frac{4}{5},\frac{5}{6},\frac{1}{1}$$

The length of Farey sequences increases only modestly with i. and is approximately given as

$$3(i/\pi)^2 \approx 0.304 \text{ x } i^2$$

The above approximation is good as i gets larger. The lengths of f(i) for $4 \leq i \leq 32$ in is shown in figure 1. The

Manuscript received January 5, 2009
Manuscript revised January 20, 2009

use of quaternionic Farey fractions is preferred in this work, since they have the proven advantage that, combining many quaternion transformations is more numerically stable than combining many matrix transformations. A novel feature of this work is that the encrypted text can be represented in numbers instead of the conventional alphabets. Also, the number of secondary keys (which are used for transforming the given plain text into cipher text) that can be generated using the primary key is large and hence more is the confusion. All these effects, prevents the hackers from breaking the encryption using the conventional approach of letter frequencies.

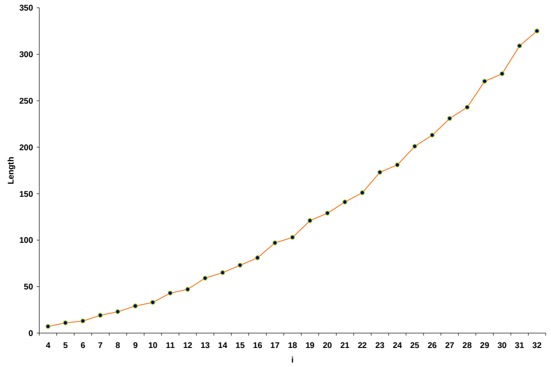


Figure 1 Variation of Farey length for different i

3. EXPERIMENTATION

Cryptographic attacks are designed to subvert the security of cryptographic algorithms, and they are used to decrypt data without prior access to a key. To take care of common crypto attacks present on a data, a quaternionic [6] Farey fraction based encryption process is proposed in this work. The proposed encryption scheme has the ability to specify a 'key' or 'password' of some kind, and have the encryption method alter itself such that each key or password produces a different encrypted output, which requires a unique 'key' or 'password' to decrypt. The block diagram of the proposed Encryption process used in generating the cipher text is shown in appendix 1. The first step involves the generation of key/coefficient of quaternion using Farey fractions. The Farey fraction sequence of order 'i', F(i), consists of all fractions with values between '0' and '1' whose denominators do not exceed 'i', expressed in lowest terms and arranged in order of increasing magnitude. All the fundamental properties of quaternions are made use of in this step and a Farey sequence (represented by a sequence of completely reduced fractions between '0' and '1') of order 'n' is used. Since, homogenous matrices are the standard 3D representations the equivalent rotation matrix representing a quaternion is performed as shown in figure 1. Following this step, a number of secondary keys are generated and the final form of cipher text is produced. Farey sequence can be used to generate the co-efficient for the quaternion and the same can be used as a main key for generating the sequence of secondary keys.

3.1 ENCRYPTION PROCESS

The encryption process can be illustrated as follows:

Step 1:

Let n1 is an integer. Then the Farey sequence is represented as F(n1). Let a1/b1 be the kth element, the same will be used as the first coefficient of the quaternion. Similarly, the Farey sequence can be generated for the integer numbers n2, n3, and n4 and kth element for all these sequence can be determined. Let assume that the kth element of n2 is a2/b2, the kth element for n3 is a3/b3 and the kth element of n4 is a4/b4.

Step 2:

Let w, x, y and z are the co-efficients of the quaternion generated as follows:
w = ASCII value of (numerator(a1) + denominator(b1)
x = ASCII value of (numerator(a2) + denominator(b2)
y = ASCII value of (numerator(a3) + denominator(b3)
z = ASCII value of (numerator(a4) + denominator(b4)
This process increases the confusion.

Step 3:

Key Generation:

- In order to create more confusion, a 16 key is created using the combination of alpha numeric characters or Farey fractions. These combinations enable to create millions of key combinations, which certainly make it impossible for the hackers to guess the key combinations.

Step 4:

- Once the key is created, a random number is generated in the range 1 and 16 and the corresponding character is selected and the same is used as the first co-efficient of the quaternion. This process is repeated four times to generate four random numbers between 1 and 16 and the corresponding characters are selected and used as quaternion or the co-efficient of the super complex number.

Step 5:

Assume that **q** is the primary key consisting of four alphanumeric characters or Farey fractions (q = (w,x,y.z)). These quaternion can be converted into rotational matrix as in equation (1). Equation (1) can be used for manipulation in both encryption and decryption process.

$$f(q) = \begin{pmatrix} w^2+x^2-y^2-z^2 & 2(xy-wz) & 2(xz+wy) \\ 2(xy+wz) & w^2-x^2+y^2-z^2 & 2(yz-wx) \\ 2(xz-wy) & 2(yz+wx) & w^2-x^2-y^2+z^2 \end{pmatrix} \text{------(1)}$$

Step 6:
Initial key or primary key is generated as q = (w,x,y,z) where w,x,y,z are the independent co-efficient of the quaternion. Using the primary key **'q'**, series of secondary keys are generated with the help of rotation matrix. These sequences of secondary keys are used for encryption process.

3.2 THE DECRYPTION PROCESS

The decryption process is reverse of the Encryption process.

Key Generation

Key K_B: This key is of size N, where 'N' represents number of Plain text blocks

Keys K_1, K_2, K_3, K_4 ………… K_N: These keys are generated using the natural numbers with modulo arithmetic, by taking right shift (or left shift) of specified digits.

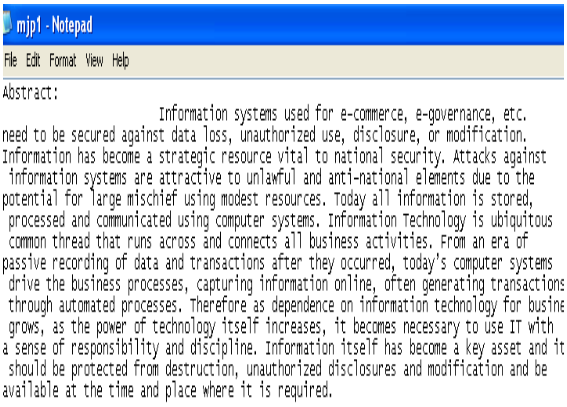
Key Kc: This key is used to join the blocks. Hacking difficult by randomly selecting the cipher blocks to obtain the final plain text.

4. RESULTS AND DISCUSSION

4.1 Result

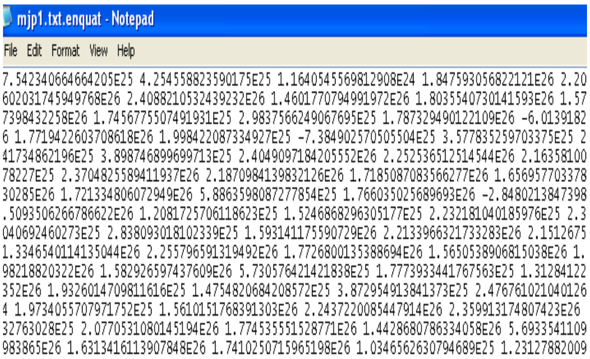
4.1.1 Encrypted result

The input plain text and its encrypted data using the steps illustrated in section is shown in figure 2 and 3 respectively.



```
Abstract:
                         Information systems used for e-commerce, e-governance, etc.
need to be secured against data loss, unauthorized use, disclosure, or modification.
Information has become a strategic resource vital to national security. Attacks against
 information systems are attractive to unlawful and anti-national elements due to the
potential for large mischief using modest resources. Today all information is stored,
 processed and communicated using computer systems. Information Technology is ubiquitous
 common thread that runs across and connects all business activities. From an era of
passive recording of data and transactions after they occurred, today's computer systems
 drive the business processes, capturing information online, often generating transactions
 through automated processes. Therefore as dependence on information technology for busine
 grows, as the power of technology itself increases, it becomes necessary to use IT with
a sense of responsibility and discipline. Information itself has become a key asset and it
 should be protected from destruction, unauthorized disclosures and modification and be
available at the time and place where it is required.
```

Figure 2 Input file with plain text

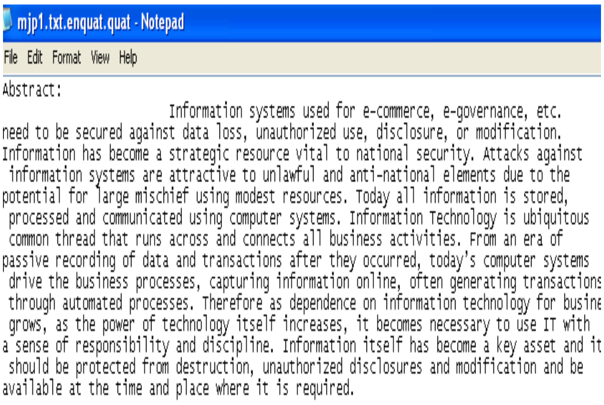


```
7.542340664664205E25 4.254558823590175E25 1.1640545569812908E24 1.847593056822121E26 2.20
602031745949768E26 2.4088210532439232E26 1.4601770794991972E26 1.8035540730141593E26 1.57
7398432258E26 1.7456775507491931E25 2.9837566249067695E25 1.787329490122109E26 -6.0139182
6 1.7719422603708618E26 1.998422087334927E25 -7.384902570505504E25 3.577835259703375E25 2
41734862196E25 3.898746899699713E25 2.4049097184205552E26 2.252536512514544E26 2.16358100
78227E25 2.3704825589411937E26 2.1870984139832126E26 1.7185087083566277E26 1.656957703378
30285E26 1.721334806072949E26 5.886359808727785 4E25 1.766035025689693E26 -2.848021384739 8
.5093506266786622E26 1.2081725706118623E25 1.5246868296305177E25 2.232181040185976E25 2.3
04069246027 3E25 2.838093018102339E25 1.593141175590729E26 2.2133966321733283E26 2.1512675
1.3346540114135044E26 2.255796591319492E26 1.7726800135388694E26 1.5650538906815038E26 1.
98218820322E26 1.582926597437609E26 5.730576421421838E25 1.777393344176 7563E25 1.31284122
352E26 1.932601470981161 6E25 1.4754820684208572E25 3.872954913841373E25 2.47676102104012 6
4 1.973405570797175 2E25 1.561015176839130 3E26 2.243722008544791 4E26 2.3599131748074 23E26
32763028E25 2.0770531080145194E26 1.774535551528771E26 1.4428680786334058E26 5.6933541109
983865E26 1.6313416113907848E26 1.741025071596519 8E26 1.0346562630794689E25 1.2312788200 9
```

Figure 3 Encrypted file with Cipher text

4.1.2 Decryption result

The Decrypted text obtained using the decryption algorithm is shown in figure 4. Performance analysis is done by comparing the resultant decrypted data with the original data.



```
Abstract:
                         Information systems used for e-commerce, e-governance, etc.
need to be secured against data loss, unauthorized use, disclosure, or modification.
Information has become a strategic resource vital to national security. Attacks against
 information systems are attractive to unlawful and anti-national elements due to the
potential for large mischief using modest resources. Today all information is stored,
 processed and communicated using computer systems. Information Technology is ubiquitous
 common thread that runs across and connects all business activities. From an era of
passive recording of data and transactions after they occurred, today's computer systems
 drive the business processes, capturing information online, often generating transactions
 through automated processes. Therefore as dependence on information technology for busine
 grows, as the power of technology itself increases, it becomes necessary to use IT with
a sense of responsibility and discipline. Information itself has become a key asset and it
 should be protected from destruction, unauthorized disclosures and modification and be
available at the time and place where it is required.
```

Figure 4 Output of Decryption

4.2 Discussion

The Proposed method implements a simple cryptosystem and is also observed to be highly secure. In this work, the properties of Farey fractions are used to

1. Generate the specified number of Farey fractions of specified length.
2. Determine the kth Farey fraction

This, in turn, is used as the coefficient of the quaternion or the key to the encryption process. The implemented crypto technique has the following advantages:

I. The transmitted key (when interrupted/intercepted) does not give any opportunity for the hackers to guess. The very reason for the same is that, the key may be numerals or even the name of a person whose date of birth can be used as a key.

II. The primary Key is not used for the encryption/ Decryption, but series of secondary keys are generated and the same is used in sequence for encryption. Similarly at the receiving end the series of Inverse keys are generated using the primary key and the same is used in sequence for the decryption process.

III. Farey fractions are used to generate the primary key, which makes more confusion for the hackers to break or interpret the code

IV. Quaternion is the super –complex number which gives multi-fold security. This work generates quaternion valued security code with the help of quaternion Farey fractions and offers the security at multi-level.

V. Quaternion provides the multiple and the variable key's length which are the essential factors for determining the degree of the security.

VI. The crypto system is highly appropriate for asymmetric–key encryption. Quaternion has the capacity to provide encryption system for the transmission of text and images.

VII. The coding process is simple enough.

VIII. The frequency analysis is almost zero and hence, it is impossible for the hackers to guess the key.

5. CONCLUSION

In this research work, the applications of Farey fractions are used to generate the specified number of Farey fractions for a specified length and the kth Farey fraction is determined. This, in turn, is used as the coefficient of the quaternion or the key to the encryption process. The encrypted code is represented in the form of floating point numbers, which makes it almost impossible to break the code using the frequency analysis. This gives high degree of confusion to the hackers and a very high provable security to the information. Further more, the key distribution problem is significantly reduced: there is no longer a need for exchanging secret keys.

REFERENCES

[1] Whitfield Diffman and Martin Hellman "New Directions of cryptography", Bulletin of the American Mathematical Society 42 (2005), 3-38; online in 2004. ISSN 0273-0979.

[2] Rolf S. Krausshar, "Generalized Analysis. Of Hyper complex numbers, Mathematics society - 2004

[3] C. C. Chang., "An Information Protection Scheme Based upon Number Theory", The Computer Journal, Vol. 30, No. 3, 1987, pp. 249-253.

[4] H. Chandrashekhar and M. Nagaraj, "Tribes of Gaussian Farey Fractions", Mathematical Student, Vol. 63, 1-4 (1994), pp.196-200.

[5] H. Chandrashekhar, "Algebraic coding theory based on Farey Fractions", Thesis Submitted to the Bangalore University for the award of the Ph. D. Degree. 1997.

[6] W. Donley Jr "Quaternionic discrete series by Joshua Holden, "Journal of Proc. Amer Math, Society, Posted Nov 12th 2002.

[7] Kim S. Lee, Huizhu Lu, D. D. Fisher, "A Hierarchical Single-Key-Lock Access Control Using the Chinese Remainder Theorem", Symposium on Applied Computing Proceedings, 1992, pp. 491 – 496.

[8] M. L Wu and T. Y. Hwang, "Access control with single key-lock", IEEE Transaction on Software Engineering, Vol. SE-10, No. 2, (1984), pp.185-191

[9] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, "Primes in P", Analysis of Mathematics, 160 (2004), pp. 781–793

[10] Thamous A berson, "Differential cryptanalysis" Anagram La, Palo Alto, CA- USA.

[11] Ronald L. Riverst, A. Shamir, and L. Adlernan. "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, volume 21, Feb. 1978, pp. 120–126.

[12]. Goldwasser and J. Kilian, "Almost all primes can be quickly certified", Proc. Annual ACM Symposium on the Theory of Computing, 1986, pp. 316–329.

[13] Sabrina De Capitani di Vimercati1, Pierangela Samarati1, and Sushil Jajodia2.: "Policies, Models, and Languages for Access Control", S. Bhalla (Ed.)
DNIS 2005, LNCS 3433, Springer-Verlag Berlin Heidelberg 2005, pp. 225–237.

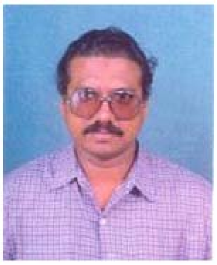
[14] Shonon C.E, "A mathematical Theory of Communication", BH System Technical Journal, July 1948, p 379.

[15] Whitfield Diffie and Martin E. Hellman. "New directions in cryptography", IEEE Transactions on Information Theory, IT-22(6), Nov 1976, pp. 644-654.

[16] Whitfield Diffman. "The first ten years of public key cryptology", Proceedings of the IEEE,76(5), May 1988, pp. 560-577.

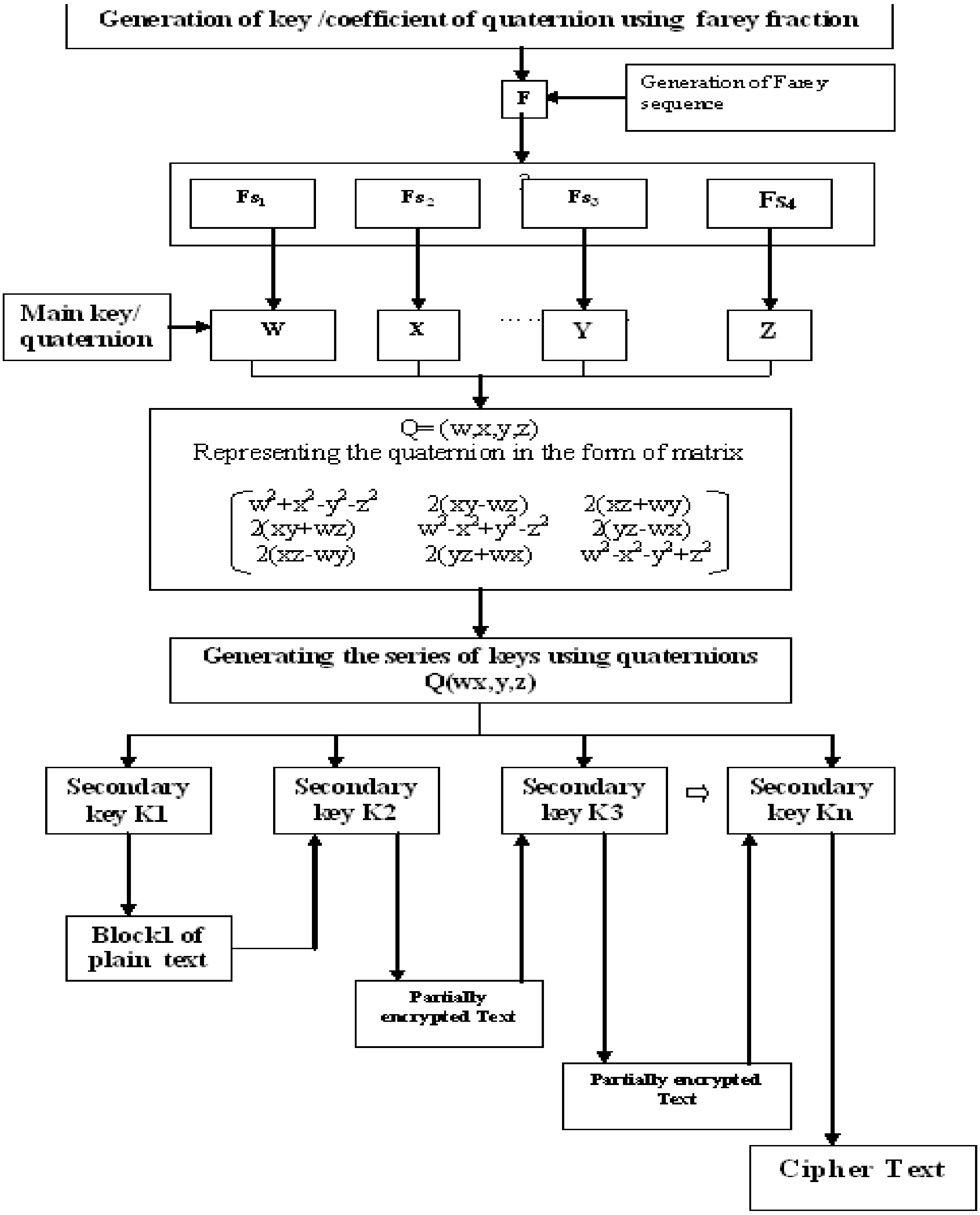
[17] Yan Sun and K. J. Ray Liu, "Scalable Hierarchical Access Control in Secure Group Communications", IEEE INFOCOM 2004.

V.Gayathri is presently a research scholar in CSE Dept. Vinayaka mission University, Salem. His areas of interest include E-Learning, Cryptography and Network Security.

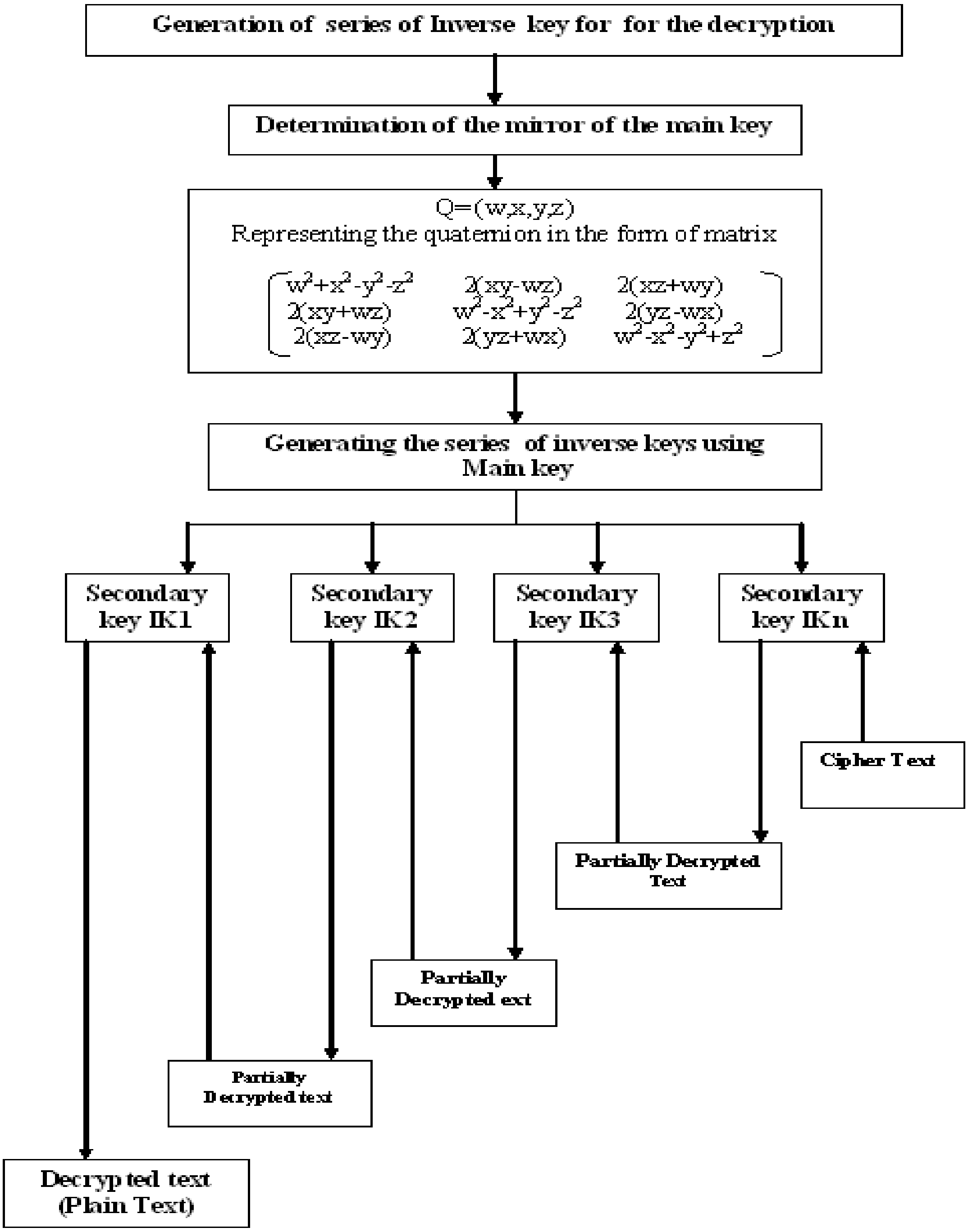


Dr.Antony Selvadoss Thanamani is presently the reader in the dept of computer science. He has published more than twenty papers in national/journals and more than ten books.

APPENDIX I


Generation of key /coefficient of quaternion using farey fraction
F
Generation of Farey sequence
Fs1
Fs2
Fs3
Fs4
Main key/ quaternion
W
X
Y
Z
Q= (w,x,y,z)
Representing the quaternion in the form of matrix
w²+x²-y²-z² 2(xy-wz) 2(xz+wy)
2(xy+wz) w²-x²+y²-z² 2(yz-wx)
2(xz-wy) 2(yz+wx) w²-x²-y²+z²
Generating the series of keys using quaternions Q(wx,y,z)
Secondary key K1
Secondary key K2
Secondary key K3
Secondary key Kn
Block1 of plain text
Partially encrypted Text
Partially encrypted Text
Cipher Text

APPENDIX 2


Generation of series of Inverse key for for the decryption
Determination of the mirror of the main key
Q=(w,x,y,z)
Representing the quaternion in the form of matrix
w2+x2-y2-z2 2(xy-wz) 2(xz+wy)
2(xy+wz) w2-x2+y2-z2 2(yz-wx)
2(xz-wy) 2(yz+wx) w2-x2-y2+z2
Generating the series of inverse keys using Main key
Secondary key IK1
Secondary key IK2
Secondary key IK3
Secondary key IKn
Cipher Text
Partially Decrypted Text
Partially Decrypted ext
Partially Decrypted text
Decrypted text (Plain Text)