Numeral Structure Base Cryptography Design to Secure Distribution of Internet Assets

U.Vijay sankar
Research Scholar / CSE,
PRIST UNIVERSITY, India

Dr.A.Arul Lawrence selvakumar
Professor & Head/CSE
Rajiv Gandhi Institute of Technology, Bangalore-32

***Abstract*-The Internet is a collection of shared resources. The present internet architecture has limited support for both securing and identifying shared Internet resources. As a result, resource exhaustion does occur due to inefficiently scaling systems, selfish resource consumption and malicious attack. 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 based cryptography schemes for secure sharing of internet and intranet resources without global protocol redeployment or architectural support. Quaternionic Farey fractions are used to achieve rotations/orientations in three dimensions. The 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.**

***Keywords*- Number Theory, Quaternion, FareyFractions, Cryptography**

I. INTRODUCTION

Rapid growth of electronic communication leads to the issues like information security. Message exchanged worldwide are publicly available through the computer networks, which must be confidential and protected against malicious users. 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.1] This chapter gives the motivation which triggered to secure the secrets from the malicious users, the concepts of cryptography and the organizations of various chapters for achieving the same.

II. MOTIVATION

Cryptography is the study of message secrecy. In modern times, it has become a branch of information theory, as the mathematical study of information and especially its transmission from place to place. The noted cryptographer Ron Rivest [2] has observed that "cryptography is about communication in the presence of adversaries", which neatly captures one of its unique aspects as a branch of engineering, and differences from, for instance, pure mathematics. It is a central part of several fields: information security and related issues, particularly, authentication, and access control. One of cryptography's primary purposes is hiding the meaning of messages, but not usually their existence. Cryptography also contributes to computer science, particularly in the techniques used in computer and network security for such things as access control and information confidentiality. Cryptography is also used in many applications encountered in everyday life; examples include security of ATM cards, computer passwords, and electronic commerce all depend on cryptography.

It is necessary to secure the secrets secret, in this context, we need to have a cryptosystem which is provably secure and it should give a great deal of security. Number theory provided immense of application to cryptography using the same a highly secured system can be devised. Cryptography can be used to provide confidentiality using encryption methods and can also provide data integrity, authentication and non-repudiation. We purpose to deploy number systems based cryptography schemes for secure sharing of internet and intranet resources without global protocol redeployment or architectural support. Quaternionic Farey fractions are used to achieve rotations/orientations in three dimensions. The 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. The three distinct notions of security models namely cooperative, selfish and malicious users are uniformly taken care in this work. The techniques proposed in this paper can help in increasing the accuracy and completeness of Internet topology discovery and can leverage existing protocol and hardware features, and thus can be implemented easily on present day’s Internet.

III. ROLE OF NUMBER THEORY IN CRYPTOGRAPHY

Number theory is the branch of pure mathematics concerned with the properties of numbers in general, and integers in particular, as well as the wider classes of problems that arise from their study. Number theory may be subdivided into several fields, according to the methods used and the type of questions investigated the term "arithmetic" is also used to refer to number theory. [3]This is a somewhat older term, which is no longer as popular as it once was. Number theory used to be called the higher arithmetic, but this too is dropping out of use. Nevertheless, it still shows up in the names of mathematical fields. Number systems plays very important role in the field of cryptography.

In addition to elementary number theory, increasing use has been made of algebraic number theory and arithmetic algebraic geometry. Cryptosystems is also make use arithmetic geometry where elliptic factorization uses elliptic and hyper- elliptic curves.[4] Some of the most important applications of number theory on cryptosystems are number field sieves method for factoring large integers and the Quaternion which gives multifold security in the cryptography.[5]

The area of the research is to use the applications of the quaternion to secure the secrets using the concept called cryptography. One of the most important applications of modern mathematics in our current times is the use of cryptography in securing our network systems of communications. Although the idea dates back to ancient times only after the appearance of the RSA system can one start to build a really safe way to transmit data over long distances via internet? The backbone of the RSA system is Fermat's Little Theorem in number theory.

IV PROPERTIES OF QUATERNION

Quaternions were discovered by William Rowan Hamilton of Ireland in 1843. Hamilton was looking for ways of extending complex numbers (which can be viewed as points on a plane) to higher spatial dimensions. He could not do so for 3-dimensions, but 4-dimensions produce quaternion. According to a story he told, he was out walking one day with his wife when the solution in the form of equation i2 = j2 = k2 = ijk = -1 suddenly occurred to him; he then promptly carved this equation into the side of nearby Brougham bridge (now called Broom Bridge) in Dublin.

This involved abandoning the commutative law, a radical step for the time. Vector algebra and matrices were still in the future. Not only this, but Hamilton had in a sense invented the cross and dot products of vector algebra. Hamilton also described a quaternion as an ordered four-element multiple of real numbers, and described the first element as the 'scalar' part, and the remaining three as the 'vector' part. If two quaternion with zero scalar parts are multiplied, the scalar part of the product is the negative of the dot product of the vector parts, while the vector part of the product is the cross product. But the significance of these was still to be discovered.

Hamilton proceeded to popularize quaternion with several books, the last of which, Elements of Quaternions, had 800 pages and was published shortly after his death. Even by this time there was controversy about the use of quaternion. Some of Hamilton's supporters vociferously opposed the growing fields of vector algebra and vector calculus (developed by Oliver Heaviside and Willard Gibbs among others), maintaining that quaternion provided a superior notation. While this is debatable in three dimensions, quaternion cannot be used in other dimensions (though extensions like octonions and Clifford algebras may be more applicable). In any case, vector notation had nearly universally replaced quaternion in science and engineering by the mid-20th century.

Today, quaternions see use in computer graphics, control theory, signal processing and orbital mechanics, mainly for representing rotations/orientations in three dimensions. For example, it is common for spacecraft attitude-control systems to be commanded in terms of quaternion, which are also used to telemeter their current attitude. The rationale is that combining many quaternion transformations is more numerically stable than combining many matrix transformations Hamilton used addition symbol in the Cartesian representation of a complex number. Let us consider the complex number a+ib, which is somewhat misleading, since a real and purely imaginary number cannot be directly added together arithmetically. A more suitable representation might be as an ordered pair of real numbers (a, b), together with a set of manipulation rules that define how to perform operations like addition and multiplication of these pairs.

V FAREY FRACTIONS AND PROPERTIES

The Farey fractions, named after the British geologist John Farey (1766-1826), provide an example. The Farey fraction sequence of order i, F(i),consists of all fractions with values between 0 and1 whose denominators do not exceed i, expressed in lowest terms and arranged in order of increasing magnitude.

For example, F (6) is 0/1, 1/6, 1/5, ¼, 1/3, 2/5, 1/2, 3/5,2/3.3/4,4/5.5/6,1/1

In mathematics, a Farey sequence of order n is the sequence of completely reduced fractions between 0 and 1 which, when in lowest terms, have denominators less than or equal to n, arranged in order of increasing size. Each Farey sequence starts with the value 0, denoted by the fraction 0/1, and ends with the value 1, denoted by the fraction 1/1. Farey observed that the fractions in such sequences are the mediants of their adjacent fractions. The mediant of n1/d1 and n2/d2 is (n1 + n2)/ (d1 + d2) which looks like a naive attempt to add fractions. Farey sequences have a number of other interesting and useful properties. The Farey sequence is a well-known concept in number theory, whose exploration has lead to a number of interesting results. However, from an algorithmic point of view, very little is known. In particular, the only problem that appears to be investigated is that of generating the entire sequence for a given n.

A sequence of fractions can be interpreted as integer sequences in a number of ways.[6] Since the numerators and denominators show distinctive patterns, a natural method is to separate a sequence of fractions into two sequences, one of the numerators and one of the denominators as in:

Fn (6) = 0, 1, 1, 1, 1, 2, 1, 3, 2, 3, 4, 5, 1
Fd(6) = 1, 6, 5, 4, 3, 5, 2, 5, 3, 4, 5, 6, 1

The Farey sequence Fn for any positive integer n is the set of irreducible rational numbers a/b with 0<a<b<=n and (a, b)==1 arranged in increasing order The first few are

F1 = {0/1, 1/1}
F2 = {0/1, 1/2, 1/1}
F3 = {0/1, 1/3, 1/2, 2/3, 1/1}
F4 = {0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1}
F5 ={0/1,1/5,1/4,1/3,2/5,1/2,3/5,2/3,3/4,4/5,1/1}

For given integer n and k, we can generate the k-th element of the Farey sequence of order n (often called the k-th order statistic [2]) and the same can be used for the different practical applications. Suppose to list of all fractions between 0 and 1 inclusive, whose denominator does not exceed a given number n.

When n is 1, the list contains just 0 and 1, that is, 0/1 and 1/1.
When n is 2, the list contains 0/1, 1/2, 1/1.
When n is 3, the list contains 0/1, 1/3, 1/2, 2/3, 1/1.
When n is 4, the list contains 0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1.

Note that we have excluded 2/4, as being equivalent to 1/2. A list like this is known as a Farey sequence. Different lists are distinguished by their "order", that is, the number n which represents the largest denominator. The following diagram shows all Farey sequences from order 1 to 6.

```
[0/1,                                          1/1]
[0/1,                  1/2,                    1/1]
[0/1,      1/3,        1/2,        2/3,         1/1]
[0/1,   1/4, 1/3,    1/2,    2/3, 3/4,          1/1]
[0/1,1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5,       1/1]
[0/1, 1/6, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 1/1]
```

Inspection of this illustration reveals many curious properties of Farey sequences. We'll just look at a couple. For every sequence of order >= 2, the fraction 1/2 stands in the middle. Any two terms equidistant from 1/2 are complementary, that is to say, they add up to 1. Looking at the Farey sequence of order 6, we see that

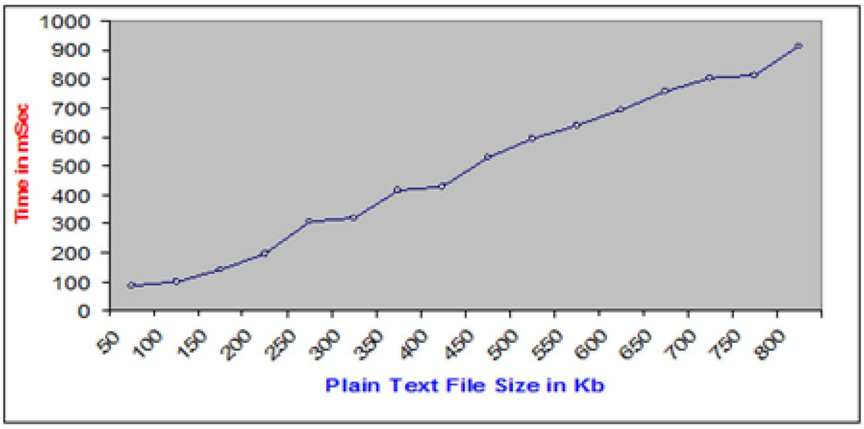
- 2/5 and 3/5 are both one away from 1/2. Their sum is 1.
- 1/3 and 2/3 are both two away from 1/2. Their sum is 1.
- 1/4 and 3/4 are both three away from 1/2. Their sum is 1.
- 1/5 and 4/5 are both four away from 1/2. Their sum is 1.
- 1/6 and 5/6 are both five away from 1/2. Their sum is 1.
- 0/1 and 1/1 are both six away from 1/2. Their sum is 1.

VI. RESULT ANALYSIS USING QUATERNIONIC FAREY FRACTIONS

The Proposed method implements a simple cryptosystem and is also observed to be highly secure and has the following advantages:

- The length of the primary key is 16 digits; the same is used to generate sequence of secondary keys. The 16 digit key is reduced to 8 digits by selecting randomly and same is used to generate the farey sequences. This may create lot of confusion to the hackers to find the actual key used for the encryption and decryption process.
- The 8 digit key is divided in to 4 blocks each consisting of 2 –digits, farey sequence is generated for each block and the same is used as parameter or key co-efficient for the quaternion.
- 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.
- 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.
- Farey fractions are used to generate the primary key, which makes more confusion for the hackers to break or interpret the code
- 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.

- Quaternion provides the multiple and the variable key's length which are the essential factors for determining the degree of the security.
- The crypto system is highly appropriate for symmetric–key encryption. Quaternion has the capacity to provide encryption system for the transmission of text and images.
- The coding process is simple enough.
- The frequency analysis is almost zero and hence, it is impossible for the hackers to guess the key.
- The time complexity function tells us how much computational steps we will have to perform to solve that problem. Often, the exact amount of steps involved is of no particular interest to us, but the order of magnitude of the problem is. Such a concept is extremely important in the development of an algorithm that needs to be executed on a computer. There are often many ways to solve a problem and one would strive to find an algorithm for which the order of the time complexity function called the time complexity is minimal. If the order of the function becomes large, a slightly bigger version of the problem (composed of only a few more elements) might require an enormous amount of extra computations. Those take up processor time, hence the name "time complexity". In even simpler terms: it shows us how fast the amount of time required to solve a problem grows when the size of the problem grows. The time complexity of a problem is the number of steps that it takes to solve an instance of the problem as a function of the size of the input (usually measured in bits), using the most efficient algorithm. The figure below shows the time taken to encrypt a given text file.



VI. CONCLUSION

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 test results obtained establishes that encryption and decryption are fast and therefore makes its implementation feasible. The fact that, unlike conventional encryption techniques, the symmetric key generated in this research work, is not sequence of number and instead can also just represent the name of the person. This name may be known only to the sender and the friendly receiver. Also, the same name is not used directly, but, rather the date of birth of the specified person will be used as key for the encryption and decryption process. This gives high degree of confusion to the hackers and a very high provable security to the information.

The need of quaternion and farey fraction is to analyze and implement cryptography which provides high security using the properties of the quaternion. Using immense applications of number theory we can device a cryptosystem which provides high level of confusion and it makes the hackers impossible to break the code. Here, the cryptosystem is devised using the properties of quaternion and farey fractions. The applications of number theory contribute greatly for providing provably secure cryptosystem.

ACKNOWLEDGMENT

I would like to thank and acknowledge Dr.A.Arul L.S, for his continuous support and guidance. I would also like to acknowledge all the support rendered by my colleagues, family and friends.

REFERENCES

[1]. WhitfielDiffman and Martin Hellman "New Directions of cryptography"Bulletin of the American Mathematical Society 42 (2005), 3-38; online in 2004. ISSN 0273-0979.
[2]. 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.
[3]. Neal Koblitz "A Course in Number Theory and Cryptography (Graduate Texts in Mathematics) "
[4]. Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman "An Introduction to Mathematical Cryptography"

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

[6]. H.Chandrashekar, "Algebraic coding theory based on Fare Fractions".

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

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

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

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

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

[12]. William Stallings, "Cryptography and Network Security", Third Edition, Pearson Education, 2003

[13]. AtulKahate, "Cryptography and Network Security", Tata McGrawHill, 2003

[14]. Jonathan Katz and Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols (Chapman & Hall/Crc Cryptography and Network Security Series)