International Research Journal of Computer Science (IRJCS)
Issue 2, Volume 2 (February 2015)
ISSN: 2393-9842
www.irjcs.com

ENCRYPTION AND DECRYPTION PROCESS USING QUATERNION AND FAREY FRACTIONS FOR SECURE TRANSMISSION

U. Vijay Sankar
Ph.D., Research Scholar/CSE
PRIST University, INDIA.

Dr.A.Arul Lawrence Selvakumar
Professor & Head/CSE
RGIT, Bangalore, INDIA

Abstract -Encryption and Decryption technique using quaternion and farey fractions can be used for secure transmission over networks that are vulnerable to attacks. The farey fractions can be used to generate the primary key and same is used by quaternion. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The process of converting a plain text to a cipher text is called is called *enciphering* or *encryption* and the reverse process is called *deciphering* or *decryption*. One of cryptography's primary purposes is hiding the meaning of messages, but not usually their existence. Encryption is perfectly secret if and only if an adversary cannot distinguish between two plain text even if the computing resource of the adversary is unlimited. Good cryptographic systems should always be designed so that they are as difficult to break as possible. It is possible to build systems that cannot be broken in practice.

Keywords: Number Theory, Quaternion, Farey Fractions, Cryptography

I. Introduction

Encryption and Decryption technique using quaternion and farey fractions can be used for secure transmission over networks that are vulnerable to attacks. The farey fractions can be used to generate the primary key and same is used by quaternion to generate four dimensional encryption keys which significantly eliminates the risk of eavesdropping.

II. Concept of Cryptography

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message we want to send is the *plain text* and the disguised message is called as *cipher text.* The process of converting a plain text to a cipher text is called is called *enciphering* or *encryption* and the reverse process is called *deciphering* or *decryption*.

In modern times, the cryptography 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 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, One of cryptography's primary purposes is hiding the meaning of messages, but not usually their existence. Encryption is perfectly secret if and only if an adversary cannot distinguish between two plain text even if the computing resource of the adversary is unlimited. Cryptography also contributes to computer science, particularly in the techniques used in computer and network security for such things as access control, data integrity 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.

III. Strength of Cryptographic Algorithms

Good cryptographic systems should always be designed so that they are as difficult to break as possible. It is possible to build systems that cannot be broken in practice (though this cannot usually be proved). This does not significantly increase system implementation effort; however, some care and expertise is required. There is no excuse for a system designer to leave the system breakable. Any mechanisms that can be used to circumvent security must be made explicit, documented, and brought into the attention of the end users.

In theory, any cryptographic method with a key can be broken by trying all possible keys in sequence. If using **brute force** to try all keys is the only option, the required computing power increases exponentially with the length of the key. A 32 bit key takes 2^32 (about 10^9) steps. This is something any amateur can do on his/her home computer. A system with 40 bit keys (e.g. US-exportable version of RC4) takes 2^40 steps - this kind of computing power is available in most universities and even smallish companies. A system with 56 bit keys (such as DES) takes a substantial effort, but is quite easily breakable with special hardware. The cost of the special hardware is substantial but easily within reach of organized criminals, major companies, and governments. Keys with 64 bits are probably breakable now by major governments, and will be within reach of organized criminals, major companies, and lesser governments in a few years. Keys with 80 bits may become breakable in future. Keys with 128 bits will probably remain unbreakable by brute force for the foreseeable future. Even larger keys are possible; in the end we will encounter a limit where the energy consumed by the computation, using the minimum energy of a quantum mechanics operation for the energy of one step, will exceed the energy of the mass of the sun or even of the universe.

However, key length is not the only relevant issue. Many ciphers can be broken without trying all possible keys. In general, it is very difficult to design ciphers that could not be broken more effectively using other methods. Designing your own ciphers may be fun, but it is not recommended in real applications unless you are a true expert and know exactly what you are doing.

One should generally be very wary of unpublished or secret algorithms. Quite often the designer is then not sure of the security of the algorithm, or its security depends on the secrecy of the algorithm. Generally, no algorithm that depends on the secrecy of the algorithm is secure. Particularly in software, anyone can hire someone to disassemble and reverse-engineer the algorithm. Experience has shown that a vast majority of secret algorithms that have become public knowledge later have been pitifully weak in reality.

The key lengths used in public-key cryptography are usually much longer than those used in symmetric ciphers. There the problem is not that of guessing the right key, but deriving the matching secret key from the public key. In the case of RSA, this is equivalent to factoring a large integer that has two large prime factors. In the case of some other cryptosystems it is equivalent to computing the discrete logarithm modulo a large integer (which is believed to be roughly comparable to factoring). Other cryptosystems are based on yet other problems.
Hence the strength encryption algorithm depends on :

The range of key: - the larger the key range makes it difficult or some time impractical to crack the key using brute force attack.

Time taken for encryption and decryption:-a good encryption algorithm should very less time to encrypt and decrypt.

Cipher text produced: - the cipher data has to be scrambled to an extent that it makes the cryptanalysis impossible.

IV. Various Attacks on Cryptosystems

Cryptanalysis is the art of deciphering encrypted communications without knowing the proper keys. There are many cryptanalytic techniques. Some of the more important ones for a system implementer are described below.
Man-in-the-middle attack: This attack is relevant for cryptographic communication and key exchange protocols. The idea is that when two parties are exchanging keys for secure communications (e.g., using Diffie-Hellman, an adversary puts himself between the parties on the communication line. The adversary then performs a separate key exchange with each party. The parties will end up using a different key, each of which is known to the adversary. The adversary will then decrypt any communications with the proper key, and encrypt them with the other key for sending to the other party. The parties will think that they are communicating securely, but in fact the adversary is hearing everything.
Timing Attack: This very recent attack is based on repeatedly measuring the exact execution times of modular exponentiation operations. It is relevant to at least RSA, Diffie-Hellman, and Elliptic Curve methods.
Attacks against Implementations: Many systems fail because of mistakes in implementation. Some systems don't ensure that plaintext is destroyed after it's encrypted. Other systems use temporary files to protect against data loss during a system crash, or virtual memory to increase the available memory; these features can accidentally leave plaintext lying around on the hard drive. In extreme cases, the operating system can leave the keys on the hard drive. One product we've seen used a special window for password input.

The password remained in the window's memory even after it was closed. It didn't matter how good that product's cryptography was; it was broken by the user interface.

V. Encryption and Decryption

Encryption and Decryption mechanism has been used to protect communication since ancient times. In cryptography encryption is the process of transforming information to make it unreadable to anyone except those possessing special knowledge , usually referred to as a key. Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now used in protecting many kinds of civilian systems such as internet e-commerce, mobile telephone networks and bank ATMs. Encryption is also used in digital rights management to restrict the use of copyrighted material and in software copy protection to prevent against reverse engineering and software piracy.

5.1 Cryptography with Quaternion and Farey Fractions

The block diagram of Encryption process used in generating the cipher text is shown in figure 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 quaternion 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. The encryption process can be illustrated as follows:

5.2 GENERATION OF KEY USING FAREY FRACTIONS

Step 1:

In order to create more confusion, a 16 key is created using the combination of numeric characters. These numeric characters are used to generate the farey sequence and the same is used to generate the co-efficients of the quaternion or the primary key. These combinations enable to create millions of key combinations, which certainly make it impossible for the hackers to guess the key combinations.

Step 2:

Once the key is created, a random number is generated in the range 1 and 16 and the corresponding number is selected This process is repeated eight times to generate eight random numbers between 1 and 16 and the corresponding numbers are selected and used to generate the farey sequence which in turn used as the coefficient of the quaternion.

Step 3:

Let n1 is an integer. Then the Farey sequence is represented as F(n1). Let a1/b1 be the k^{th} 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 k^{th} element for all these sequence can be determined. Let assume that the k^{th} element of n2 is a2/b2, the k th element for n3 is a3/b3 and the k^{th} element of n4 is a4/b4.

Step 4:

Let w, x, y and z are the co-efficients of the quaternion generated as follows:

w = ASCII value of numerator (a1) + ASCII value of denominator(b1)

x = ASCII value of numerator (a2) + ASCII value of denominator(b2)

y = ASCII value of numerator (a3) + ASCII value of denominator(b3)

z = ASCII value of numerator (a4) + ASCII value of denominator(b4)

This process increases the confusion.

Step 5:

Let assume that **q** is the primary key consist of four alphanumeric characters or Farey fractions (q= (w,x,y.z)). These quaternion can be converted in to rotational matrix as shown below, so that same can be used for manipulation in both encryption and decryption process.

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

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.

Encryption Process

- Let assume that **q** is the primary key consist of four alphanumeric characters or farey fractions (q= (w,x,y.z)). These quaternion can be converted in to rotational matrix as shown below, so that same can be used for manipulation in both encryption and decryption process..

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

Initial key or primary key 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 shown above.

- In this, the primary key is not directly used for the manipulation instead sequence of secondary keys are generated and the same is used for encryption process. The sequence secondary keys are

- qs1= (ws1,xs1,ys1,zs1)

  = (0, $w^2+x^2-y^2-z^2$, 2(xy-wz), 2(xz+wy)

  qs2= (ws2, xs2,ys2,zs1)

  = (0, 2(xz-wy), 2(yz+wx), $w^2-x^2-y^2+z^2$)

  qs3= (ws3, xs,ys3,zs3)

  = (0, $w^2+x^2-y^2-z^2$, 2(xy-wz), 2(xz+wy))

qs4= (ws4,xs4,ys4,zs4)

= ($w^2+x^2-y^2-z^2$,0,, 2(xy-wz), 2(xz+wy)

qs5= (ws5, xs5,ys5,zs5)

= (2(xz-wy), 0, 2(yz+wx), $w^2-x^2-y^2+z^2$)

qs6= (ws6, xs6,ys6,zs6)

= ($w^2+x^2-y^2-z^2$, 0, 2(xy-wz), 2(xz+wy))

qs7= (ws7,xs7,ys7,zs7)

= ($w^2+x^2-y^2-z^2$, 2(xy-wz), 0, 2(xz+wy)

qs8= (ws8, xs8,ys8,zs8)

= (2(xz-wy), 2(yz+wx),0, $w^2-x^2-y^2+z^2$)

qs9= (ws9, xs9,ys9,zs9)

= ($w^2+x^2-y^2-z^2$, 2(xy-wz), 0, 2(xz+wy))

qs10= (ws10,xs10,ys10,zs10)

= ($w^2+x^2-y^2-z^2$, 2(xy-wz), 2(xz+wy,0)

qs11= (ws11, xs11,ys11,zs11)

= (2(xz-wy), 2(yz+wx), $w^2-x^2-y^2+z^2$, 0)

qs12= (ws12, xs12,ys12,zs12)

= ($w^2+x^2-y^2-z^2$, 2(xy-wz), 2(xz+wy), 0)

- The plain text is divided into sequence of block, each block consist of a 3 X 3 matrix consist of nine characters. Each block of plain text is encrypted by the sequence of secondary keys. ie the first block of plain text is encrypted by **qs1** and the output of the same is taken by the next secondary key qs2 and the output(cipher text) is given as input to the third secondary key qs3 and the process is repeated and final encrypted (cipher text) text of the first block(plain text) is created.

- Above encryption process is repeated till the all the blocks of plain text converted in to cipher text.

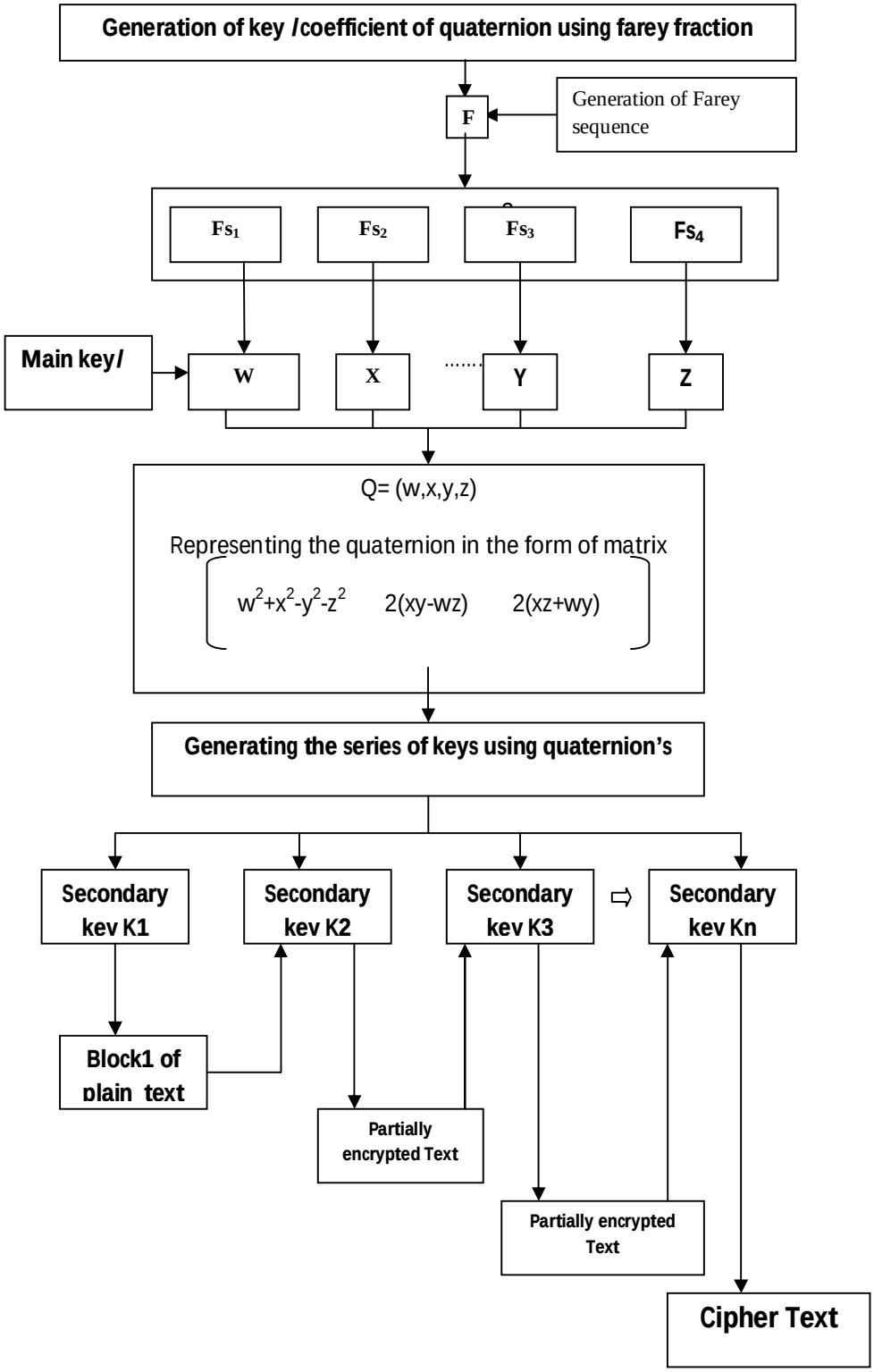

Fig: Encryption process

DECRYPTION PROCESS

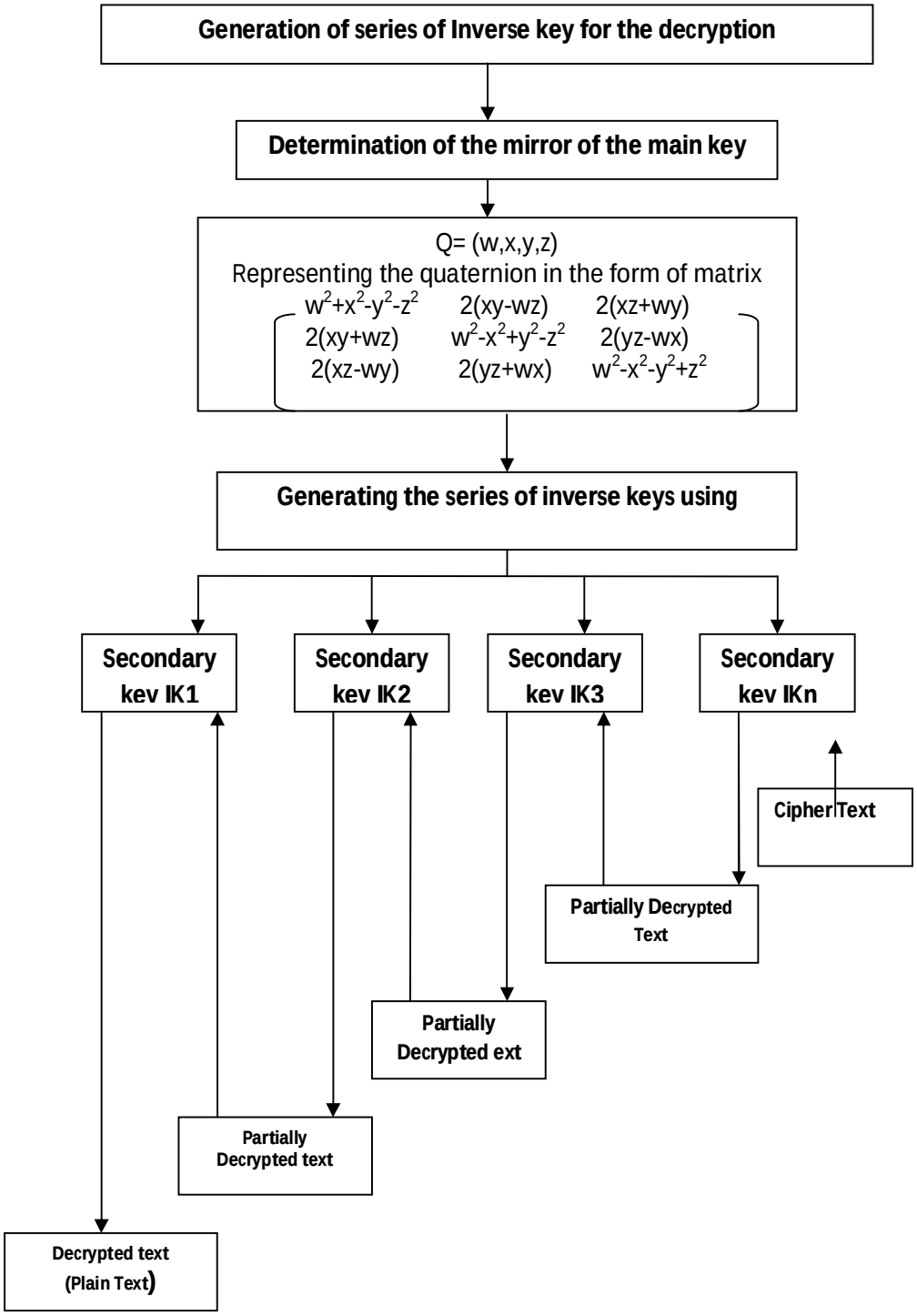

Fig: Decryption Process

- The important point to be noted here is that, the encrypted text are represented in the form of numerals (floating point numbers) instead of alphabetic character. This complicates the hackers to break the code by tracing the letter frequencies. Storing the encrypted text may require more space because each encrypted character is stored in the form of numerals but the same can be reduced by storing the encrypted text in the form of the four variables.

- Decryption process starts with generating inverse key. In order to generate the inverse key first the mirror of the key is determined then the determinant of the key is determined (since the key is represented in the form rotational matrix) for example, let q is the primary key, the mirror of the key is determined as follows.

$$q = \begin{pmatrix} K[0][0] & k[0][1] & k[1][2] \\ K[1][0] & k[1][1] & k[1][2] \end{pmatrix}$$

The mirror of q can be written as

$$Mq = \begin{pmatrix} m[0][0] & m[0][1] & m[1][2] \\ m[1][0] & m[1][1] & m[1][2] \end{pmatrix}$$

Where m[0][0] = k[1][1] *k[2][2] - k[2][1]* k[1][2]

m[0][1] = k[1][0] *k[2][2] - k[2][0]* k[1][2] and so on.

Therefore inverse of key q Iq = mq / determinant of q

Similarly Inverse key for all the secondary keys are determined namely isq1, isq2, isq3……..isq12.These inverse key are used for the decryption process.

The first cipher block is taken and the same is multiplied with the inverse secondary key isq1 to give the partially decrypted block namely ipdb1 and the same is multiplied by *isq2* to yield *ipdb2***.** This process is repeated till the inverse key **isq12** multiplies the partially decrypted block *pdb12***.** Finally *ipdb12* is the decrypted block. This process is repeated for all the cipher block to get the decrypted blocks.

VI. CONCLUSION

In this work the applications of farey fractions are used to generate the specified number of farey fractions for the specified length and the k^{th} farey fraction is determined in turn the ASCII value of the same is used as the coefficient of the quaternion. Or the key to the encryption process. This may create lots of confusion and diffusion to the hackers. The plain text is encrypted using the key which generated by farey fractions and quaternion. Decryption is taking place by determining the inverse of the key. This may make the hackers work very much complicated impossible to break the code to determine the secret. Hence the securing the secrets is very much possible by using the immense application of number theory.

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] Whitfiel 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] 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. 560577.
[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 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] Atul Kahate, "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) "

