Secure Joint Resources Using Quaternion and Complex 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 – 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. . The objective of this research work is to analyze and implement highly secure cryptography scheme using the properties of quaternion Farey fractions. 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. 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.

Keywords: Number Theory, Quaternion, Farey Fractions, 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. 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.

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 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. 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.

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.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 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.

IV.OPERATIONS ON QUATERNION

- **Arithmetic operations on Quaternion:**

Addition and subtraction of quaternion proceed component-wise:

$$q = (a,\ b,\ c,\ d) = a\ + ib\ + jc\ + kd,$$
$$p = (x,\ y,\ z,\ w) = x\ + iy\ + jz\ + kw,$$

$$q+p = (a+x,b+y,c+z,d+w) = (a+x) + i(b+y) + j(c+z) + k(d+w),$$
$$q-p = (a-x,b-y,c-z,d-w) = (a-x) + i(b-y) + j(c-z) + k(d-w).$$

- **Multiplication by a Real Number**

The multiplication of quaternion's could be deduced from the following multiplication table:

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

These products form the quaternion group of order 8, Q_8.
Multiplication by a real number x has the effect of scaling each component:
Q = (a, b, c, d) = a +ib +jc +kd,
xq = qx= (xa,xb,xc,xd) = xa +i(xb) +j(xc) +k(xd).

❖ Alternative Representation

In addition to the Cartesian and quadruple representations

q = (a,b,c,d) = a+ib+jc+kd,

there is an alternative way to represent a quaternion. We separate the real part **a** from the purely imaginary (or *pure*) part **ib+jc+kd.** It turns out that it is natural to represent the pure part by the vector (b,c,d), since (as we shall see) i,j, and k act like orthogonal unit vectors. We put q = (a,**v**), where **v**=(b,c,d).

Then

q+p = (a,**v**) + (x,**u**) = (a+x,**v**+**u**),

where `+' represents the usual operations of real, respectively vector, addition.

❖ Conjugation and Absolute Value

The conjugate is given by

$q = (a, b, c, d) = a+ib+jc+kd,$
$q^* = (a,-b,-c,-d) = a-ib-jc-kd.$

Or, in the alternative representation,

q = (a,**v**),
q^* = (a,-**v**).

The absolute value is given by extending Pythagoras's theorem to four dimensions, and is equal to the square root of the product of a number and its conjugate:

|q| = SQRT($a^2+b^2+c^2+d^2$) = SQRT(qq^*).

❖ Multiplication of Quaternion

q = (a,b,c,d),
p = (x,y,z,w),
qp
= (a+ib+jc+kd)(x+iy+jz+kw)
= a(x+iy+jz+kw)
+ib(x+iy+jz+kw)
+jc(x+iy+jz+kw)
+kd(x+iy+jz+kw)

= ax+iay+jaz+kaw
+ibx -by+kbz-jbw
+jcx-kcy -cz+icw
+kdx+jdy-idz -dw

= (ax-by-cz-dw,
ay+bx+cw-dz,
az-bw+cx+dy,
aw+bz-cy+dx)

This can be re-written much more conveniently using the alternative representation of real number and 3-vector as follows:

p = (x,**u**), q(a,**v**)
qp = (ax-**v**.**u**, a**u**+x**v** + **v**X**u**).

[Where X is the vector cross-product.] With this representation, it becomes obvious that quaternion multiplication is not commutative, since the cross-product of the vectors is not commutative.

- Multiplying Quaternion

Since a unit quaternion represents an orientation in 3D space, the multiplication of two unit quaternion will result in another unit quaternion that represents the combined rotation. Amazing, but it's true. Given two unit quaternion

Q1=(w1, x1, y1, z1);
Q2=(w2, x2, y2, z2);

A combined rotation of unit two quaternion is achieved by

Q1 * Q2 =(w1.w2 - v1.v2, w1.v2 + w2.v1 + v1*v2)

where v1= (x1, y1, z1)
v2 = (x2, y2, z2)

and both . and * are the standard vector dot and cross product.

However an optimization can be made by rearranging the terms to produce
w=w1w2 - x1x2 - y1y2 - z1z2
x = w1x2 + x1w2 + y1z2 - z1y2
y = w1y2 + y1w2 + z1x2 - x1z2
z = w1z2 + z1w2 + x1y2 - y1x2

Of course, the resultant unit quaternion can be converted to other representations just like the two original unit quaternion. This is the real beauty of quaternion - the multiplication of two unit quaternion in 4D space solves gimbal lock because the unit quaternion lie on a sphere. Be aware that the order of multiplication is important. Quaternion multiplication is not commutative, meaning
q1 * q2 does not equal q2 * q1

- **Squaring**

Note that the above rule for multiplication means that we have

$$q^2 = (a^2 - \mathbf{v}.\ \mathbf{v},\ 2a\mathbf{v})$$

Because the cross-product of any vector with itself is zero.

- **Inverse and Division**

Recall that $qq^* = q^*q = |q|^2$,
thus $(qq^*)/(|q|^2) = (q^*q)/(|q|^2) = 1$,
giving the (both left and right) inverse of q to be $q^{-1}=q^*/(|q|^2)$.

We can use the inverse to define division. However, one has to be careful what is meant by division. We could define either

$q/p = qp^{-1}$, or $q/p = p^{-1}q$.

- **Real and Complex Subspaces**

Quaternion's of the form

$(a,0,0,0) = a$

are just real numbers. Similarly, quaternions of any of the three following forms:

$(a,b,0,0) = a+ib$,
$(a,0,c,0) = a+jc$,
$(a,0,0,d) = a+kd$.

are just equivalent complex numbers, and are closed under the operations of addition and multiplication.
Pure quaternion (q=ib+jc+kd), however, are not closed since the dot product of the vector parts contributes to the real part of a product.

V. CONVERSION FROM QUATERNION

To be able to use quaternion effectively, we shall eventually need to convert them to some other representation. You cannot interpret keyboard presses as quaternion, can you? Well, not yet.

- **Quaternion to Matrix**

The Direct3D allow rotations to be specified as matrices, this is probably the most important conversion function, since homogenous matrices are standard 3D representations. The equivalent rotation matrix representing a quaternion is

$$\begin{array}{llll} \text{Matrix} = [& w^2 + x^2 - y^2 - z^2 & 2xy - 2wz & 2xz + 2wy \\ & 2xy + 2wz & w^2 - x^2 + y^2 - z^2 & 2yz - 2wx \\ & 2xz - 2wy & 2yz + 2wx & w^2 - x^2 - y^2 + z^2] \end{array}$$

Using, property of unit quaternion that $w^2 + x^2 + y^2 + z^2 = 1$, we can reduce matrix to

$$\begin{array}{llll} \text{Matrix} = [& 1 - 2y^2 - 2z^2 & 2xy - 2wz & 2xz + 2wy \\ & 2xy + 2wz & 1 - 2x^2 - 2z^2 & 2yz - 2wx \\ & 2xz - 2wy & 2yz + 2wx & 1 - 2x^2 - 2y^2] \end{array}$$

- Quaternion to Axis Angle

To change a quaternion to a rotation around an arbitrary axis in 3D space, we do the following:

If the axis of rotation is (ax, ay, az)
and the angle is theta (radians)
then the angle= 2 * acos(w)
ax= x / scale
ay= y / scale
az= z / scale
where scale = sqrt $(x^2 + y^2 + z^2)$

Another variation is that the scale = sin(acos(w)). They may be equivalent, though It is not tried to find the mathematical relationship behind them. If the scale is 0, it means there is no rotation so unless you do something, the axis will be infinite. So whenever the scale is 0, just set the rotation axis to any unit vector with a rotation angle of 0.

VI. Encryption and Decryption

Encryption and Decryption mechanism has been used to protect communication since ancient times. In cryptography encryption does the process of transforming information to make it unreadable to anyone except those possess 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.

6.1 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-efficient 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.

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

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..

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

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.

VII.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 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. 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) "