PYTHAGOREAN TRIPLE BASED CRYPTOGRAPHY SYSTEM FOR INFORMATION SECURITY

[1]R. Adeoye, [2]O. Adetan and [3]O.D. Alowolodu
[1]Department of Computer Engineering, Ekiti State University, Ado Ekiti, Nigeria
[2]Department of Electrical & Electronic Engineering, Ekiti State University, Ado Ekiti, Nigeria
[3] Department of Computer Science, Federal University of Technology, Akure, Nigeria

[1]adeoye.richard.ar@gmail.com [2]oadetan@gmail.com [3]funsoalowodu@yahoo.com

***Abstract*—Information is compromised at a high rate as there is significant increase in the number of hackers or attackers. The aim of compromising information is to attack confidentiality, integrity and availability of the message. The paper implements the security of information using Pythagorean triple based cryptographic system which makes use of the new Pythagorean triple algorithm. This cryptographic system makes use of symmetric cryptography that only the sender and the receiver have in order to secure information. It makes use of a secret key P and Q where $P > Q$. The secret keys; P and Q are used in the Pythagorean triple cryptographic system to devise the solutions of the Pythagorean triple. The Java programming language has been chosen to perform the encryption and decryption of message in this work. The Pythagorean triple cryptographic system is a more secure cryptography system which prevents cryptanalytic and bruth-force attack to a large extent**

***Keywords*—cryptographic system, symmetric cryptography, bruth-force attack, cryptanalytic attack**

I. INTRODUCTION

Security has been defined as the quality or state of being secure or to be free from. Information security in the world at large has been very essential as it enables individuals, organization and groups from different backgrounds to secure files, data, programs etc. The Committee on National Security Systems (CNSS) defines information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information. Information security allows confidentiality, integrity and availability. The work done by [1] makes use of the new Pythagorean triple algorithm in which $p > q$ (one of them is odd and the other even). There is only one fundamental solution $(x. y, z)$. However, using the new Pythagorean triple algorithm formulas, this definition can be re-stated to state that; for any numbers p and q (one of them is odd and the other even) there are at least two fundamental solutions (x_1, y_1, z_1) and (x_2, y_2, z_2), but there are also special cases when even three fundamental solutions are possible (x_1, y_1, z_1) ,$(x_2, y_2, z_2$and (x_3, y_3, z_3).

1.1 An Overview of Information Security

The history of information security begins with computer security. The primary threats to security were physical theft of equipment, espionage against the products of the systems and sabotage. The concept of data hiding technologies whose aim is to solve modern network security, quality of services control, and secure communications, has been seen as a cost-effective alternative to other means of data security, which does not require protocol modifications, and is compatible with existing standards of multimedia compression and communications [2].

Over the years, a number of security approaches have been developed that help in managing information security. There have been only a few isolated (less-well known) approaches to consider the socio-technical aspects of information systems security management [3]. Although these approaches help in managing security, there is a need for information security approaches to provide a holistic modeling support which can be integrated into modern information development approaches [3]. Most of the modern approaches to information security employ cryptography.

According to [4], a message in readable form is known in cryptographic terms as a plaintext. The process of masquerading a message in a way to hide its substance is referred to as encryption and the resulting message is known as ciphertext. The reverse process which is decryption takes ciphertext, C as input and restores the original plaintext P. The encryption function E operates on P to produce C:

$$E(P) = C \qquad (1)$$

In the reverse process, the decryption function D operates on C to produce P:

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$D(C) = P \qquad (2)$$

A cryptographic algorithm called a cipher is a mathematical function that is used for encryption and decryption requires the cryptosystem kept secret. This method is called security by obscurity and is used only in very specific cases. Also, it was ascertained that Cryptography provides security through a number of mathematical transformations that can be proven to be mathematically secure provided some optimum conditions are satisfied [5]. Cryptography is not the silver bullet to solve all information security issues and should be used in conjunction with good security practices [6]. Cryptographic protocols are a vital component of information Security [7] as a means of securing modern networks against would-be attackers by providing data integrity, encryption and authentication to network traffic at the transport layer [8].

2. METHODOLOGY

New Pythagorean Triple uses Symmetric algorithms to encrypt and decrypt a message using the same key. A Pythagorean triple represent an ordered triple of the type $(x.y,z \in Z^3)$ such that $(x^2 + y^2 = z^2)$[8]. The conventional way of interpretation of the above mentioned equation is that there is one solution (x_1, y_1, z_1) to the aforementioned equation [9]. One of the most known methods of generating a pythagorean triple is the Euclid's formula which is a fundamental formula for Pythagorean triples for given arbitrary pair of positive integers *p* and *q* where $p > q$. The formula states that the integers derived from Euclid's formula as given in equation (1) represents a Pythagorean triple.

$$\left.\begin{array}{c} x = p^2 - q^2 \\ y = 2pq \\ z = p^2 + q^2 \end{array}\right\} \qquad (3)$$

Through the New Pythagorean Triple algorithm we can extend the definition of the Pythagorean Theorem which states that for any p and q, there is only one fundamental solution$(x.y,z)$. Using the New Pythagorean Triple algorithm formulas, this definition can be re-stated to: for any numbers p and q there are at least two fundamental solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) or(x_1, y_1, z_1), (x_2, y_2, z_2) and (x_3, y_3, z_3) .Based on these solutions we can easily create the encryption and decryption key that can be used in a simple symmetric cryptosystem.
Let us have $x^2 + y^2 = z^2$and $\gcd(x, y) = 1$. There is a number z so that:

$$\left.\begin{array}{c} z = x + u \\ z = y + v \end{array}\right\} \qquad (4)$$

where $\gcd(x, y) = 1$ and $\gcd(y, v) = 1$.

where gcd is the greatest common divisor.

$$\left.\begin{array}{c} x + u = y + v \\ x - v = y - u \end{array}\right\} \qquad (5)$$

Let us make $y - u = x - v = \lambda$, then:

$$\left.\begin{array}{c} x = v + \lambda \\ x = u + \lambda \end{array}\right\} \qquad (6)$$

If we replace x in equation 2 with equation 3 we get (7) as:

$$z = u + v + \lambda \qquad (7)$$

Equations 3 and 4 are then given as:

$$\left.\begin{array}{c} x = v + \lambda \\ y = u + \lambda \\ z = u + v + \lambda \end{array}\right\} \qquad (8)$$

Equation (6) represents the new fundamental solutions to the Pythagorean Theorem. If we replace these expressions in (6) with $x^2 + y^2 = z^2$, we have the expression given in equation 7 as:

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$(u + \lambda^2) + (v + \lambda^2) = (u + v + \lambda)^2 \qquad (9)$$

from which, after further extension, we have:

$$\lambda^2 = 2vu \qquad (10)$$

Values of v and u will be selected that way so that they determineλ, out of which we derive the Pythagorean fundamental solutions given as:

$$\left.\begin{array}{c} v = 2p^2 \\ u = q^2, v > u, \gcd(p, q) = 1 \end{array}\right\} \qquad (11)$$

If u and v are replaced in equation 8 we have:

$$\left.\begin{array}{c} \lambda^2 = 4p^2q^2 \\ \lambda = \pm 2pq \end{array}\right\} \qquad (12)$$

If equations (11) and (12) are replaced in equation (6) we have:

$$\left.\begin{array}{c} x = 2p^2 \pm 2pq \\ y = q^2 \pm 2pq \\ z = 2p^2 + q^2 \pm 2pq \end{array}\right\} \qquad (13)$$

From the conventional definition of Pythagorean triple, it results that only one fundamental solution (x, y, z) exists for which p and q. Based on equation (13), the previous definition is re-defined to: for any numbers p and q, there are at least two fundamental solutions(x_1, y_1, z_1) and (x_2, y_2, z_2) or(x_1, y_1, z_1), (x_2, y_2, z_2) and (x_3, y_3, z_3) which can be expressed in the form of New Pythagorean Triple formulas in equations (14) as:

$$\left.\begin{array}{c} x_1 = 2p^2 + 2pq \\ x_2 = 2p^2 - 2pq \\ x_3 = 2pq \\ \\ y_1 = q^2 + 2pq \\ y_2 = q^2 - 2pq \\ y_3 = p^2 - q^2 \\ \\ z_1 = 2p^2q^2 + 2pq \\ z_2 = 2p^2 + q^2 - 2pq \\ z_3 = p^2 + q^2 \end{array}\right\} \qquad (14)$$

3. RESULTS AND DISCUSSIONS

3.1 Data Encryption and Decryption

This section shows how we can encrypt and decrypt a text by using the New Pythagorean Triple Algorithm formulas for creating the key. Let us mark with *m* the plaintext whereas with *k* the key and with *c* the encrypted message (cipher text). For any message to be encrypted, equation (15) is used.

$$c = m + k(mod 26) \qquad (15)$$

In order to decrypt a message, equation (14) is used

$$m = c - k(mod 26) \qquad (16)$$

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table 1: The English alphabets

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**

To show how the key is going to be created. The numbers p and q are put within the New Pythagorean Triple Algorithm formulas given below to create the key to a mod of 26. I can then freely create the encryption key in the form: $x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3$. To encrypt the plain text EKITI STATE for example as shown in Table 2.

Table 2: Message encoding for the word "ekiti state"

E	**K**	**I**	**T**	**I**	**S**	**T**	**A**	**T**	**E**
4	**10**	**8**	**19**	**8**	**18**	**19**	**0**	**19**	**4**

If odd numbers $p = 5$ and $q = 3$ are to be used as the keys, the new Pythagorean triple algorithm equations becomes:

$$\left.\begin{aligned} x_1 &= 2*5^2 + 2*5*3 = 80 \\ y_1 &= 3^2 + 2*5*3 = 39 \\ z_1 &= 2*5^2 + 3^2 + 2*5*3 = 89 \end{aligned}\right\} \quad (17)$$

$$\left.\begin{aligned} x_2 &= 2*5^2 - 2*5*3 = 20 \\ y_2 &= 3^2 - 2*5*3 = -21 \\ z_2 &= 2*5^2 + 3^2 - 2*5*3 = 29 \end{aligned}\right\} \quad (18)$$

$$\left.\begin{aligned} x_3 &= 2*5*3 = 30 \\ y_3 &= 5^2 - 3^2 = 16 \\ z_3 &= 5^2 + 3^2 = 34 \end{aligned}\right\} \quad (19)$$

Hence the key ($x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3$) to a modular arithmetic of 26 will be:

$$(80,39,89,20,-21,29,30,16,34)(mod\ 26) = (2,13,11,20,5,3,4,16,8)$$

The message will then be encrypted using equation (15).

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table 3: Message encryption using odd numbers p and q

e	**k**	**i**	**T**	**i**	**s**	**t**	**a**	**t**	**e**
4	**10**	**8**	**19**	**8**	**18**	**19**	**0**	**19**	**4**
2	**13**	**11**	**20**	**5**	**3**	**4**	**16**	**8**	**2**
6	**23**	**19**	**13**	**13**	**21**	**23**	**16**	**1**	**6**
G	**X**	**T**	**N**	**N**	**V**	**X**	**Q**	**B**	**G**

Hence, the cipher text is ***GXTNNVXQBG***. The recipient of the encrypted message must have the pair of number $(p, q) = (5, 3)$. The received message can now be decrypted, by finding the key. The secret number is the pair of number $(p, q) = (5, 3)$ and the receiver calculates the key from the pair of numbers using the new Pythagorean Triple algorithm formulas. The recipient then calculates the key $x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3$as explained earlier. The message will then be decrypted using equation (16) as shown in Table 4.

Table 4: Message decryption using odd numbers p and q

g	**x**	**t**	**N**	**n**	**v**	**x**	**q**	**b**	**g**
6	**23**	**19**	**13**	**13**	**21**	**23**	**16**	**1**	**6**
2	**13**	**11**	**20**	**5**	**3**	**4**	**16**	**8**	**2**
4	**10**	**8**	**19**	**8**	**18**	**19**	**0**	**19**	**4**
E	**K**	**I**	**T**	**I**	**S**	**T**	**A**	**T**	**E**

The original text is then retrieved back to be 'EKITISTATE'.

If even numbers are to be used $p = 4\ and\ q = 2$ as the keys, using the New Pythagorean Triple algorithm formulas, the expression in equations (18-20) will give:

$$\left.\begin{aligned} x_1 &= 2 * 4^2 + 2 * 4 * 2 = 48 \\ y_1 &= 2^2 + 2 * 4 * 2 = 20 \\ z_1 &= 2 * 4^2 + 2^2 + 2 * 4 * 2 = 52 \end{aligned}\right\} \qquad (18)$$

$$\left.\begin{aligned} x_2 &= 2 * 4^2 - 2 * 4 * 2 = 16 \\ y_2 &= 2^2 - 2 * 4 * 2 = -12 \\ z_2 &= 2 * 4^2 + 2^2 - 2 * 4 * 2 = 20 \end{aligned}\right\} \qquad (19)$$

$$\left.\begin{aligned} x_3 &= 2 * 4 * 2 = 16 \\ y_3 &= 4^2 - 2^2 = 12 \\ z_3 &= 4^2 + 2^2 = 20 \end{aligned}\right\} \qquad (20)$$

The procedure follows the same explanation given above. The key ($x_1, y_1, z_1, x_2, y_2, z_2, x_3, y_3, z_3$) to a modular arithmetic of 26 will be:

$$(48,16,16,-12,12,52,20,20)(mod\ 26) = (22,16,16,20,14,12,0,20,20)$$

Table 4: Message encryption using even numbers p and q

e	k	i	t	i	s	t	a	t	e
4	10	8	19	8	18	19	0	19	4
22	16	16	20	14	12	0	20	20	22
0	0	24	13	22	4	19	20	13	0
A	A	Y	N	W	E	T	U	N	A

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Hence, the cipher text is ***AAYNWETUNA***. The recipient of the encrypted message must have the pair of number $(p, q) = (4, 2)$ .The received message can then be decrypted, by finding the key. In this case, the secret number is the pair of number$(p, q) = (4, 2)$.

Table 5: Message decryption using even numbers p and q

a	a	y	n	w	e	t	u	n	a
0	0	24	13	22	4	19	20	13	0
22	16	16	20	14	12	0	20	20	22
4	10	8	19	8	18	19	0	19	4
E	K	I	T	I	S	T	A	T	E

3.2 Experimental results

The results of the test described above is shown in Figure 1 from the sender's side.

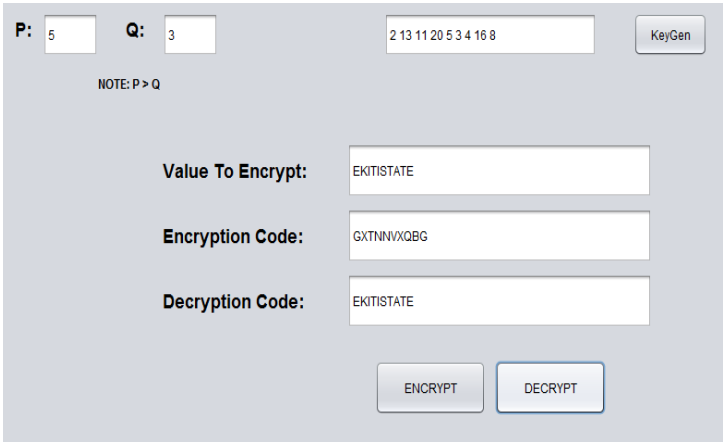

Figure 1: The senders side

4. CONCLUSION

Different techniques have been used in the past which could not provide absolute security of information in store or in transit. There are motivations to develop system which make use of stronger algorithms to keep information more safe. The main purpose of this work was achieved by studying (Pythagorean Triple based Cryptography) to develop a cryptographic information security framework. The Pythagorean Triple based Cryptosystem has been described which is a promising next generation symmetric information security system. The proposed system have been implemented and tested and the result shows that the proposed cryptosystem performed better in information security. The result of this work can however be used in the military, electronic and communications engineering fields where the exact recipients of information/message is allowed to have access to the message.

REFERENCES

[1] Artan, L and R. Bujar, "Data Encryption and Decryption using new Pythagorean Triple Algorithm", *Proceedings of the World Congress on Engineering*. London, United Kingdom, Vol 1, July 2-4, 2014

[2] Lovoshynovskiy S., F. Deguillaume, O. Koval and T. Pun. "Information Theoretic Data Hiding", *International Journal of Image and Graphics*. Vol 5(1), pp 1-31, January 2005.

[3] Siponen M.T, "An Analysis of the Recent Information Security Development Approaches", University of Oulu, Finland , Pp 101-124, 2001.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

[4] Alowolodu O.D, B.K. Alese, A.O Adetunmbi, O.S. Adewale, and O.S. Ogundele,. "Elliptic Curve Cryptography for Securing Cloud Computing Applications". International Journal of Computer Applications (0975 – 8887) Volume 66– No.23, March, 2013

[5] Schneier B., "The Non-Security of Secrecy", .http://www.schneier.com October, 2004

[6] Schneier B. and N. Ferguson,"Practical Cryptography", Wiley Publishing, Pp 185-222, April, 2003.

[7] Allen C., T. Dierks, "The tls Protocol Version", ACM digital library, RFC Editor, United State of America, 1999.

[8] Clark, P.L."Pythagorean Triples". Number Theory. 2009. http://math.uga.edu/ pete/numbertheory2009.html

[9] Bernhart F. and H. L. Price. "Heron's Formula, Descartes Circles, and Pythagorean Triangles", Number Theory, Cornell University library, January, 2007.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500