Journal, Advances in Mathematical & Computational Sciences
Vol. 8 No. 1, March 2020
www.mathematics-computationaljournal.info

Article Citation Format
Adigun A. A., Ibrahim M. A., & Ale T. O. (2020): Review of Pythagorean Triple Based Cryptography System for Information Security. Journal of Advances in Mathematical & Computational Sc. Vol. 8, No. 1. Pp 89-96.

Article Progression Time Stamps
Article Type: Research Article
Manuscript Received 6th Jan, 2020
Final Acceptance: 1st March, 2020

Review of Pythagorean Triple Based Cryptography System for Information Security

[1]Adigun A. A. [2]Ibrahim M. A., & [3]Ale T. O.
Department of Information and Communication Technology
Osun State University
Oshogbo, Nigeria
E-mail: [2]fempej2013@gmail.com, [1]ibrahima@uniosun.edu.ng, [3]peacegain2@gmail.com
Phone:[1] +2348134249446; [2]+2348033749081

ABSTRACT

Data is compromised at a high rate as there is a significant increase in the number of hackers, intruders or attackers. Hacking information aims to attack confidentiality, integrity and availability of the message. The paper implementations make use of secret key P and Q as a solution to the Pythagorean triple algorithm. JavaScript, HTML and CSS are the programming language chosen to perform the encryption and decryption of messages. Pythagorean triple based cryptographic system is a secured cryptography system which prevents cryptanalytic and brute-force attack to a large extent.

Keywords*:* Pythagorean, Triple Based Cryptography, Systems, Information Security

1. INTRODUCTION

Information security in the world at large has been very crucial as it helps organizations, individuals and groups to secure files, data, programs, e.t.c (Blake, 2013). 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 (Adetan, 2016). Pythagorean triple based method 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, 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)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) (Ochieng, et al. 2019). The longest side of the triangle is called the "hypotenuse", so the formal definition is: In a right-angled triangle, the square of the hypotenuse is equal to the sum of the squares of the other two sides. If we know the lengths of two sides of a right-angled triangle, we can find the length of the third side (Benson, 2014).
A "Pythagorean Triple" is a set of positive integers, **a**, **b** and **c** that fits the rule:

$a^2 + b^2 = c^2$ where **c** represents the length of the hypotenuse; **a** and **b** represents the length of the other two sides of a right-angle triangle.$a^2 + b^2 = c^2$ (Ganesh , 2018).

Menezes, et. al, (2016) presented a security protocol that provides secure access to application-level proxy services. Their protocol is designed to interact with a proxy to Kerberos and to facilitate porting services that rely on Kerberos to wireless devices. The work of Hogea, (2012) focuses on security solutions for mobile user devices. Unfortunately, their work uses asymmetric cryptography and is hence too expensive for the environments. The work of Czerwinski et al. (2010) also relies on asymmetric cryptography for authentication in which when the private key is lost or hacked by the hackers can be used to access all the hidden documents.

Savu, (2014) discussed the issues of bootstrapping security devices. Their solution requires physical contact of the new device with a master device to imprint the trusted and secret information. Zhou and Hass (2017) secured ad hoc networks using asymmetric cryptography that still leaves a space for the intruders to have access to some part of the information encrypted. Carman. et al, (2011) analyzed a wide variety of approaches for key agreement and key distribution in sensor networks; and the overhead of these protocols on a variety of hardware platforms.
Nilam, (2015) suggested a Secure Information Transferring System Using Color Cryptography but could not solve the problem of information security.

2. METHODOLOGY

The PTBCS uses Symmetric algorithms to encrypt and decrypt a message using the same key. A Pythagorean triple represents an ordered triple of the type (*x, y, z*). There are many ways of generating Pythagorean triples. One of the most known methods is the Euclids formula 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 below:

$x = p^2 - q^2$
$y = 2pq$
$z = p^2 + q^2$

Represent a Pythagorean triple.

Another approach for generating Pythagorean triples lies in Newtons method which is based on the identity:

$(p^2 - q^2)^2 + (2pq)^2 \equiv (p^2 + q^2)^2$

From the identity it is clearly visible that integer solution to the equation $x^2 + y^2 = z^2$ are of the form:
$x = d(p^2 - q^2)$, $y = 2dxy$, $z = d(p^2 + q^2)$ with $p > q > 0$.

Where $(p, q) = 1$, *p* and *q* are of opposite parity (one even and one odd) and $(x, y, z) = d$. It can be proved that every Pythagorean Triple can be written in this way so, it is useful to observe *x*, *y* and *z* values. If $d = 1$ the triples are considered to be Primitive (A Pythagorean triple which is not a multiple of another is called a **primitive Pythagorean triple**.). The above mentioned equations can be extended by at least one (in special cases by two) other solutions to Pythagorean Triples.

New Pythagorean Triple Algorithm

Let us have $x^2 + y^2 = z^2$ and $gcd(x, y) = 1$. There is a number z so that:

$z = x + u$
$z = y + v$ (1)

Where $gcd(x, u) = 1$ and $gcd(y, v) = 1$. As a consequence, from the last system of equations, we have:

$X + u = y + v$
$X - v = y - u$ (2)

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

$X = v + \lambda$
$Y = u + \lambda$

If we replace x in equation 1 from 2 we get:

$z = u + v + \lambda$ (3)

Equations 2 and 3 given as:

$x = v + \lambda$
$y = u + \lambda$
$z = u + v + \lambda$ (4)

Represent the new fundamental solutions to the Pythagorean Theorem. If we replace these expressions in $x^2 + y^2 = z^2$ we will get:

$(u + \lambda 2) + (v + \lambda 2) = (u + v + \lambda)2$

From which, after further extension, we have:

$\lambda 2 = 2vu$ (5)

Values of v and u will be selected that way so that they determine λ, out of which we derive the Pythagorean Fundamental solutions:

$v = 2p2$
$u = q2, \quad v > u, \gcd(p, q) = 1$ (6)

If u and v are replaced in 5 we get:

$\lambda 2 = 4p2q2$

andthen:

$\lambda = \pm 2pq$ (7)

If now 6 and 7 are replaced in 4 we have:

$x = 2p2 \pm 2pq$
$y = q2 \pm 2pq$
$z = 2p2 + q2 \pm 2pq$ (8)

From all the definitions of Pythagorean Triple, we have our new PTBCS formulas in equation 9:

$X1= 2p^2 + 2pq$
$Y1= q^2 + 2pq$
$Z1 = 2p^2+ q^2+2pq$

$X2 = 2p2 - 2pq$
$Y2= q2 - 2pq$
$Z2= 2p^2+ q^2-2pq$

$X3= 2pq$
$Y3= P^2-q^2$
$Z3 =p^2+q^2$

3. RESULT AND DISCUSSIONS

Data Encryption and Decryption
The explanation below shows how we can encrypt and decrypt a file 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*** encrypted message (ciphertext).

If we want to encrypt a message, we will use the formula:

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

Which simply means?

To get our Cipher text = main text or plain text plus the key (mod 26) generated from the Pythagorean formula

If we want to decrypt a message, we use:

$$m = c - k(mod 26)$$

Now showing how the key is going to be created.

Journal, Advances in Mathematical & Computational Sciences
Vol. 8 No. 1, March 2020
www.mathematics-computationaljournal.info

Numbers *p* and *q* put within the New Pythagorean Triple Algorithm formulas given below to create the key.

$X1 = 2p^2 + 2pq$
$Y1 = q^2 + 2pq$ (9)
$Z1 = 2p^2 + q^2 + 2pq$

$X2 = 2p2 - 2pq$
$Y2 = q2 - 2pq$ (10)
$Z2 = 2p^2 + q^2 - 2pq$

$X3 = 2pq$
$Y3 = P^2 - q^2$ (113)
$Z3 = p^2 + q^2$

$(x1, y1, z1), (x2, y2, z2), (x3, y3, z3) \ (mod 26)$

We can 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

Table 1: Alphabets

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

To show how the key is going to be, the numbers p and q are within the New Pythagorean Triple Algorithm formulas given below are to create the key to a mod of 26. The encryption key can be in the form:

To encrypt the plain text OSUN STATE UNIVERSITY for example

If we have a plaintext, *OSUN STATE UNIVERSITY*

Table 2: Corresponding English Alphabets

O	S	U	N	S	T	A	T	E	U	N	I	V	E	R	S	I	T	Y
14	18	20	13	18	19	0	19	4	20	13	8	21	4	17	18	8	19	24

Which we want to encrypt, the system will automatically assign value to our p and q to generate the key for the encryption but, we want to make use odd numbers $p = 7$ and $q = 5$, and use them in the New Pythagorean Triple algorithm formulas:

$x1 = 2 \cdot 7^2 + 2 \cdot 7 \cdot 5 = 168$
$y1 = 5^2 + 2 \cdot 7 \cdot 5 = 95$ (1)

$z1 = 2\cdot7^2 + 5^2 + 2\cdot7\cdot5 = 193$

$x2 = 2\cdot7^2 - 2\cdot7\cdot5 = 28$
$y2 = 5^2 - 2\cdot7\cdot5 = -45$ (2)
$z2 = 2\cdot7^2 + 5^2 - 2\cdot7\cdot5 = 53$

$x3 = 2\cdot7\cdot5 = 70$
$y3 = 7^2 - 5^2 = 24$ (3)
$z3 = 7^2 + 5^2 = 74$

After we have found these values:
(168, 95, 193, 28, -45, 53, 70, 24, 74) (mod 26) = (12, 17, 11, 2, 7, 1, 18, 24, 22)

We have our key as (12, 17, 11, 2, 7, 1, 18, 24, 22)

TABLE 3: Encryption process

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

From the encryption formula we have: ciphertext = plain text + key (mod) which is c=m+k (mod 26)
Therefore to encrypt our plaintext **OSUN STATE UNIVERSITY** using odd numbers p and q

After encrypting our plain text, we have **AJFPZUSRAGETXLSKGPK** as the ciphertext sent to the recipient of the message. In the application designed, the key for p and q to decrypt the ciphertext to the phone number for decryption, and the receiver of the message calculates the key from the pair of numbers using the new Pythagorean Triple algorithm formulas. The recipient then calculates the key explained earlier. The equation **m= *c* − *k*(*mod*26)** used to decrypt the message.

Table 4: Decryption process

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

Using the same key p and q to decrypt the message plain text back.

4. EXPERIMENTAL RESULT.

The results of the test described above shown below

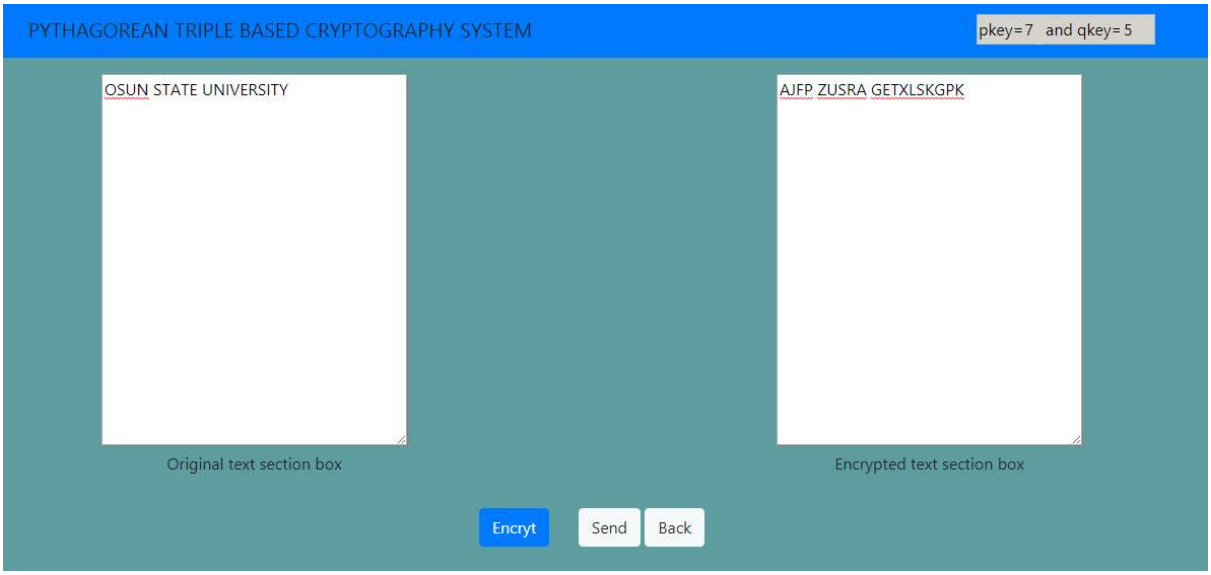

Figure 1: Encrypted Message

Figure 2: Decryption Message

5. CONCLUSION

This paper shows how the methods work and how they can explore. An asymmetric encryption algorithm was to provide more security at the communication level. The aim was to develop a Pythagorean triple based cryptographic system for information security. The choice of the programming language used is JavaScript, HTML and CSS to allow easy accessibility over the web without necessarily having to install specialized software or getting expensive hardware to run it.

REFERENCES

1. Blake (2013)Communication theory of secrecy system.*Bell Syst. Tech. J.*, 28: 656–715.
2. DomenicoBloisi and Luca Iocchi (2013). Image Based Steganography and Cryptograph, Dipartimento di Informatica e SistemisticaSapienza University of Rome, Italy
3. Gabriel J. A, (2015). "A Multivariate Polynomial-Based Post Quantum Cryptographic System for Security of Information over Enterprise Network" pp 70-72
4. Gabriel J.A., Alese B.K., Adetunmbi A.O.,Adetan C.O and Adewale O.S. (2013). "PostQuantum
5. Cryptography: A combination of Post-Quantum Cryptography and steganography". In Proceedings of the 8th International Conference for Internet Technology and Secured Transaction (ICITST-2013), technically co-sponsored by IEEE UK/RR computer Chapter, 9th – 12th December 2013, London, UK, pp 454-457.
6. Cachin .C (2012). "An Information-Theoretic Model for Steganography" in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318
7. Cohen, F (2009). A short history of cryptography. Retrieved May 4, 2009, from http://www.all.net/books/ip/Chap2-1.html