REVIEW OF PYTHAGOREAN TRIPLE BASED CRYPTOGRAPHY SYSTEM FOR INFORMATION SECURITY

A. A. ADIGUN[1], K. O. JIMOH[2], Y. O. ADEBAYO[3], M. O. KOLAWOLE[4]
[1, 2,3,4]Osun State University, Osogbo, Nigeria
[1]adepeju.adigun@uniosun.edu.ng, [2]kudirat.jimoh@uniosun.edu.ng,
[3]olajide.adebayo@uniosun.edu.ng, [4]mutairu.kolawole@uniosun.edu.ng,

Keywords: Data, Pythagorean triple based, Algorithm, Encryption and decryption, Cryptanalytic and brute-force.

Abstract: *Information security in the world at large has been very crucial as it helps organizations, individuals, and groups to secure files, data, programs. Data are 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 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. A "Pythagorean Triple" is a set of positive integers, a, b, and c that fits the rule of* $a^2 + b^2 = c^2$ *where c represents the length of the hypotenuse; a and b represent the length of the other two sides of a right-angle triangle.* $a^2 + b^2 = c.^2$ *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. JavaScript enables interactive web pages and is an essential part of web applications. The majority of websites use it, and major web browsers have a dedicated JavaScript engine to execute it. A Pythagorean triple-based cryptographic system is a secured cryptography system that prevents cryptanalytic and brute-force attacks to a large extent.*

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. [4]. Information security is 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 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$(x. y, z)$ [13]. 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),$(x_2, y_2, z_2)(x_3, y_3, z_3)$.

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 the two sides of a right-angled triangle, we can find the length of the third side.

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** represent the length of the other two sides of a right-angle triangle. $a^2 + b^2 = c^2$.

Many researchers have worked in this area and reviewed as follows:

i. Using Primitive Pythagorean Triples and Blom's Scheme in the 4-Way Handshake Wireless Security Protocol. The paper aims to propose a novel way of using Pythagorean triples along with Blom's scheme to perform raw key exchange and authentication by using a 2 stage process to do the 4-way handshake. The objectives are to use PPT's along with Blom's scheme to perform raw key exchange by use of a 4-way handshake; to analyze the cryptographic strength of random keys generated by PPT's and determined a way they can be used for wireless authentication and as raw keys for encryption in wireless security. A novel idea of using PPT's and Blom's scheme in raw key exchange and authentication using the indexing property of PPT's as a method to generate many string

sequences of infinite length. Hence, the string sequences were used for authentication keys. The experiment was run with different data sets on different variables separated by a distance of k. Since work is checking through the series, and to make sure that at least a reasonable number of variables are checked before achieve an overflow comparison. Overflow can be described as going out of bounds. The work handles overflow by treating the series as a circular series that is; when hit overflow then, the processing continues from the start. The research findings/observation for this reviewed paper, even though PPT's are random and the secret number kept secret, it is still possible for an attacker to guess the raw key being used. This is because the raw key is obtained from a table that never changes. [1]

ii. Pythagorean Triples and Cryptographic Coding with the aims to summarize the basic properties of PPTs and show that each PPTs belongs to one of six different classes. The objectives were to summarize the general properties of PPTs will be; their description in Indian texts and the context; shows that each PPT belongs to one of six different classes, and mapping an ordered sequence of PPTs into a corresponding sequence of these six classes makes it possible to use them in cryptography. Gopala-Hemachandra (GH) quadruple (g, e, f, h) was the method used to obtain the Fibonacci sequence. The results have shown that each PPT belongs to one of six distinct classes and proposed that the property be used for cryptographic applications. The research findings/observation for this paper reviewed was that the system was unable to determine the cryptographic complexity of the w-sequences. [21]

iii. Data Encryption and Decryption using Pythagorean Triple Algorithm. This work aims and objective was to create the encryption and decryption key that can be used in a simple symmetric cryptosystem, and to extend the definition of the Pythagorean Theorem. The research method was based on the New Pythagorean Triple algorithm formulas, this definition is extended to: for any numbers p and q (one of which is odd and the other even) there are at least two fundamental solutions ($x1$, $y1$, $z1$) and ($x2$, $y2$, $z2$), but there are also some special cases when we can even get three fundamental solutions ($x1$, $y1$, $z1$), ($x2$, $y2$, $z2$) and ($x3$, $y3$, $z3$). This algorithm can equally be implemented for creating the key for data encryption and decryption. The results were generated through the New Pythagorean Triple algorithm and extend the definition of the Pythagorean Theorem which states that for any p and q (one of them is odd and the other even) there is only one fundamental solution (x, y, z). The research findings/observation for this review was that no implementation or testing was carried out on this paper to prove their formula. [3]

iv. Pythagorean Triple Based Cryptography system for Information System. The aim was to implement the security of information using the Pythagorean triple-based cryptographic system which makes use of the new Pythagorean triple algorithm i.e. the use of symmetric cryptography that only the sender and the receiver have to secure information. It makes use of a secret key P and Q where P > Q. The secret keys; 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 messages in this work. These methods were used to achieve the objectives of describing the Pythagorean Triple Based Cryptosystem; studying (Pythagorean Triple based Cryptography) to develop a cryptographic information security framework, and to implement and test cryptosystem to show how it will perform 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 are allowed to have access to the message. The research findings/observation for this paper reviewed that, different techniques could provide information security but only the Pythagorean Triple Cryptography System technique is used in this paper. [20]

v. Pythagorean Triples aims to present another way of finding all the Pythagorean triples simply with the following objectives: to generate all the primitive Pythagorean triples only to calculate the primitive Pythagorean triples. Paper employed Primitive Pythagorean Triples, Tree of primitive Pythagorean triples, and Coprime as methods. All the primitive Pythagorean triples in a simple way were generated to calculate the primitive Pythagorean triples. Review shows that there is a proposed article not implemented or tested. [14].
ii. Expanded 128-bit Data Encryption Standard aimed at improving the security of DES against direct attacks; with the objectives of presenting a 128-bit approach on outdated Data Encryption Standard Cipher and to improve the defense of DES against brute force attacks. The procedure used Firstly allowed the message to be inputted and converted into binary. After that, the different keys that are going to be used for every round are produced. Next, the bits are permuted with the Modified Permuted Choice 1, after which the circular left shift is performed on the bits. Once the bits have been shifted, they are permuted

again, but this time with the use of the Modified Permuted Choice 2 so that the message can be encrypted. After 16 keys have been, the Modified Initial Permutation is used on the message and it is split into two parts. The right half goes through the Expanded Permutation to expand it. Once that is done, it is necessary to bitXOR it with the Permuted Choice 2 results that were obtained from the key. Next, the Sbox is used to substitute for the assigned values according to the addresses. Afterward, it goes through another round of permutations to reduce the value. Lastly, the value that was obtained is bitXORed with the left half of the message to obtain the first round or R1 of the plaintext. To get the value of L1, simply get the value of R-1. Many of the inner workings of the DES have been remodeled and enlarged; the Initial Permutation, PC-1, and PC-2 tables that the standard DES used can now utilize the 128-bit size of the modified DES. Because of the expansion of these tables, brute force attacks should take approximately twice as long, considering the additional steps that would be needed to decrypt the modified block cipher. Expanding the number of bits even farther beyond 128-bits. This can be either 256-bits or 512- bits. [5]

vi. Pythagorean Triples with Common Sides aimed at deriving the formulas that generate pairs of primitive Pythagorean Triples with the objectives to derive the formulas that generate pairs of primitive Pythagorean Triples with common legs; to show the process of how to determine all the primitives and non-primitive Pythagorean Triples. Euclid's general formula (primitive and non-primitive triples) is used to classify Pythagorean triples, concerning the values of the legs, and investigate different properties that might be of interest to a researcher. The only proof of formulas for Pythagorean Triples was discussed in this paper and has no control over the values of the sides of the triangle. [18]

vii. Pythagorean Triples Generator aims to develop methods that enable more flexibility in the generation process of Pythagorean Triples and to use an alternate method for generating Pythagorean Triple formulas which are different from the common method (Euclid's Method). Fibonacci's Method was adopted to describe a method for generating primitive triples for the sequence of odd natural numbers and Python Programming Language as the coding method. The results showcase flexible input values with the ability to generate all the Pythagorean triples constraint. Only Fibonacci Method was discussed. Other methods like Dickson's Method and Michael Stifel's Method were not considered. [17]

viii. Some Notes on Generalized Version of Pythagorean Triples aims to understand the new mathematical concepts of Pythagorean triples. Objectives are to construct the generalized version of the formula that generates primitive and non-primitive Pythagorean triples that depends on two positive integers k and n to determine the values of k and n that generate primitive Pythagorean triples and discuss some important results. This paper developed new results for primitive and non-primitive Pythagorean triples with detailed proofs which is a consequence of the characterization theorem and these results were provided with mathematical proof. [15]

ix. Modified DES uses Different Keystreams Based on Primitive Pythagorean Triples with the aims to have a novel approach in generating the key from the keystream for any symmetric-key algorithms using the Primitive Pythagorean Triples (PPT), and to generate keys using PPT based Keystreams. Symmetric-key algorithms using the Primitive Pythagorean Triples (PPT) were adopted to generate the key value from the keystream by both the sender and the receiver. No implementation was carried out to showcase the proposed system. [16]

x. Pythagorean Triples before and after Pythagoras aims to systematically and exhaustively discuss Pythagorean Triples; to discuss the basic problem in the field of number theory namely Pythagorean Triples, and to make a report of the origin of Pythagorean Triples. Listing of some known astonishing directions used to provide necessary and sufficient conditions with detailed proofs for the construction of Pythagorean triples. History and problem of Pythagorean Triples were discussed, but no specific formula was employed. [19]

xi. Are monochromatic Pythagorean Triples Avoidable? The aim was to tackle this problem by restricting the considered colorings to special ones satisfying certain algebraic properties and to check whether monochromatic Pythagorean triples turn out to be unavoidable. Recursive and backtracking searches were used to color all elements in Pythagorean triples within a given integer interval [1,M] without creating monochromatic. The color computation of an element m is possible if all variables in fact(m) are already colored. The results show that the monochromatic Pythagorean triples are unavoidable in [1,10000] under any 2-coloring that interval. [9]

xii. A new approach to generate all Pythagorean Triples to parameterize the Pythagorean triples and uniquely generates all of the triples. The fundamental definition of a generic Pythagorean

triple using Euclid's formula was established. The parameterization has been successfully exploited to obtain faster computations of the golden ratio and silver ratio. Data encryption and decryption were not discussed in this paper. [2]

xiii. Pythagorean Triples in Cryptography and Associated Networks was introduced with aims to generate Pythagorean Triples procedure using a coding method; to discuss what is meant by Pythagorean Triple and with encryption and decryption; to generate the Pythagorean Triples procedure using C++ Programming Language. A new procedure to obtain different sets of Pythagorean triples for the same set of input values and a procedure to encode and decode any word given in English alphabets were developed. [22]

xiv. 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.

xv. Security solutions for mobile user devices. Unfortunately, their work uses asymmetric cryptography and is hence too expensive for the environment.

xvi. 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.

xvii. Bootstrapping security devices. Their solution requires physical contact of the new device with a master device to imprint the trusted and secret information.

xviii. 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.

xix. Approaches for key agreement and key distribution in sensor networks; and the overhead of these protocols on a variety of hardware platforms.

xx. A Secure Information Transferring System Using Color Cryptography but could not solve the problem of information security.

2. METHODOLOGY

The Pythagorean Triple Based Cryptography System (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 Euclid's formula. It is a fundamental formula for Pythagorean triples for a 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 the Newton's 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:

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

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

$$x + u = y + v$$
$$x - v = y - u \qquad (2)$$

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:

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

Equations 2 and 3 given as:

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

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

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

From which, after further extension, we have:

$$\lambda 2 = 2vu \quad (5)$$

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

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

If u and v are replaced in 5 we get:

$$\lambda 2 = 4p2q2$$

And then:

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

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

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

From all the definitions of the 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

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 (cipher text).

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

$$\boldsymbol{c = m + k(mod26)}$$

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:

$$\boldsymbol{m = c - k(mod26)}$$

Now showing how the key is going to be created.
Numbers *p* and *q* are put within the New Pythagorean Triple Algorithm formulas given below to create the key.

$$X1 = 2p^2 + 2pq$$
$$Y1 = q^2 + 2p$$
$$Z1 = 2p^2 + q^2 + 2pq \quad (1)$$

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

$$X3 = 2pq$$
$$Y3 = p^2 - q^2$$
$$Z3 = p^2 + q^2 \quad (3)$$

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

We can freely create the encryption key in the form:
$x1, y1, z1, x2, y2, z2, x3, y3, z3$

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 of

odd numbers p = 7 and q = 5, and use them in the New Pythagorean Triple algorithm formulas:

$$x1 = 2 \cdot 7^2 + 2 \cdot 7 \cdot 5 = 168$$
$$y1 = 5^2 + 2 \cdot 7 \cdot 5 = 95 \quad (1)$$
$$z1 = 2 \cdot 7^2 + 5^2 + 2 \cdot 7 \cdot 5 = 193$$

$$x2 = 2 \cdot 7^2 - 2 \cdot 7 \cdot 5 = 28$$
$$y2 = 5^2 - 2 \cdot 7 \cdot 5 = -45 \quad (2)$$
$$z2 = 2 \cdot 7^2 + 5^2 - 2 \cdot 7 \cdot 5 = 53$$

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

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)
From the encryption formula we have: ciphertext = plain text + key (mod) which is $C = M + k \pmod{26}$

Therefore, to encrypt our plaintext **OSUN STATE UNIVERSITY** using odd numbers p and q

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

After encrypting our plain text, we have **AJFPZUSRAGETXLSKGPK** as the ciphertext sent to the recipient of the message.

In the application design, 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= $c - k(mod26)$**
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.

Experimental result.
The results of the test described above are shown below

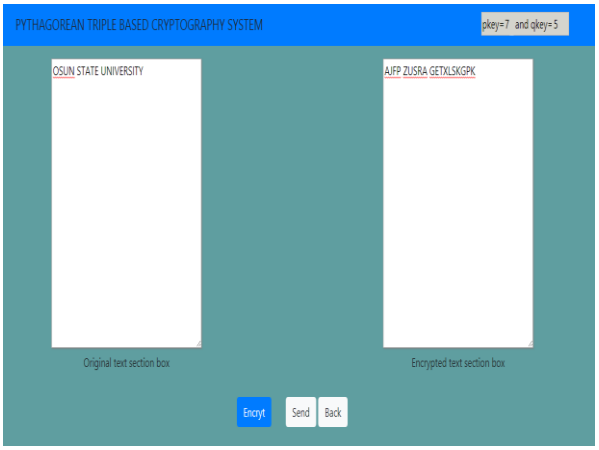

Figure 1: **Encrypted Message**

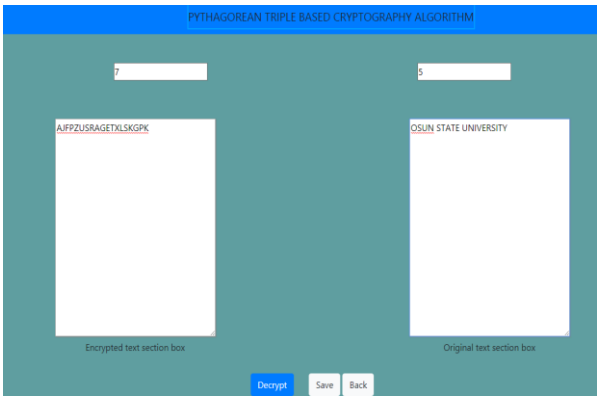

Figure 2: Decryption Message

4. CONCLUSIONS

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. JavaScript enables interactive web pages and is an essential part of web applications. The majority of websites use it and major web browsers have a dedicated JavaScript engine to execute it. This paper has many advantages over the reviewed works in encrypting and decrypting data/information. Some of the benefits are fast encryption and decryption of data, less complex

algorithm, large size of bytes generated during encryption, high secure standard of data used, and bidirectional method used in encrypting and decrypting files. The flowchart for the implementation presented as follows:

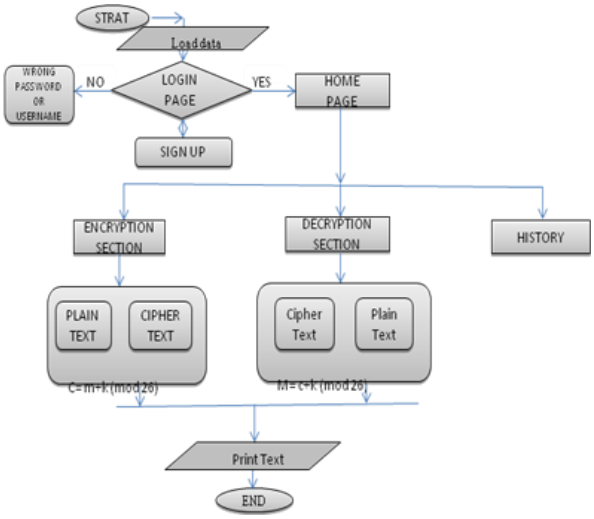

Figure 3: **System Flowchart**

5. REFERENCES

[1]. Antony Akshay - "Using Primitive Pythagorean Triples and the Blom's Scheme in the 4-Way Handshake Wireless Security Protocol", unpublished Department of Computer Science, Faculty of Graduate College, Oral Roberts University, Tulsa Okhaloma. U.S.A, 2008.

[2]. Anthony Overmars, Lorenzo Ntogramatzidis and Sitalakshmi Venkatraman - "A new Approach to generate all Pythagorean Triples". AIMS Mathematics, 4(2), pg. 242–253. DOI:10.3934/math.2019.2.242, 2019.

[3].Artan Luma and Bujar Raufi - "Data Encryption and Decryption Using New Pythagorean Triple Algorithm", Proceedings of the World Congress on Engineering. Vol I, 2014.

[4]. Blake - Communication theory of secrecy system.*Bell Syst. Tech. J.*, 28: 656–715, 2013.

[5]. Bryan F. Cruz, Keinaz N. Domingo, Froilan E. De Guzman, Jhinia B. Cotiangco, Christopher B. Hilario - "Expanded 128-bit Data Encryption Standard", International Journal of Computer Science and Mobile Computing. IJCSMC, Vol. 6, Issue 8, pg. 133 – 142, 2017.

[6].Cachin. C - "An Information-Theoretic Model for Steganography" in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 2012.

[7].Cohen, F -. A short history of cryptography. Retrieved May 4, 2009, from http://www.all.net/books/ip/Chap2-1.html, 2009.

[8]. DomenicoBloisi and Luca Iocchi- Image Based Steganography and Cryptograph, Dipartimento di Informatica e SistemisticaSapienza University of Rome, Italy, 2013.

[9]. Eliahou S., Fromentin J., Marion-Poty V., Robilliard D. - "Are Monochromatic Pythagorean Triples Avoidable", arXiv:1605.00859v1[math.CO], 2016.

[10]. Fridrich, J., Goljan, M., and Hogea, D. – Steganalysis of jpeg images: Breaking the f5 algorithm. InProc. Of In 5th International Workshop on Information Hiding, 2002.

[11]. Fridrich, Jessica, Goljan .M, and Soukal .D - "Searching for the Stego Key" Proc.SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI 5306: 70–82. Retrieved 23, January 2014.

[12]. Gabriel J. A, - "A Multivariate Polynomial-Based Post Quantum Cryptographic System for Security of Information over Enterprise Network" pp 70-72, 2015.

[13]. Gabriel J.A., Alese B.K., Adetunmbi A.O., Adetan C.O, and Adewale O.S. - "PostQuantum 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, 2013.

[14]. José William Porras Ferreira - "Pythagorean Triples", *Centro de Investigaciones Científicas, Escuela Naval de Cadetes "Almirante Padilla", Isla Manzanillo, Cartagena de Indias, Colombia, 2018.*

[15].Leomarich F. Casinillo and Emily L. Casinillo - "Some Notes on Generalized Version of Pythagorean Triples", Jurnal Riset dan Aplikasi Matematika, Vol. 4, No. 2, pg. 103 – 107, 2020.

[16]. Mani K., Devi A. - "Modified DES using Different Keystreams Based On Primitive Pythagorean Triples", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.3, No.1, pg.38-48. DOI: 10.5815/ijmsc.2017.01.04, 2017.

[17].Padavala - "Pythagorean Triples Generator", Journal of Mathematics Research; Vol. 13, No. 3, pg. 63 – 68, 2021.

[18]. Raymond Calvin Ochieng, Chiteng'a John Chikunji, and Vitalis Onyango-Otieno - "Pythagorean Triples with Common Sides", Hindawi Journal of Mathematics, Article ID 428651, 2019. https://doi.org/10.1155/2019/4286517

[19]. Ravi P. Agarwal - "Pythagorean Triples before and after Pythagoras", Department of Mathematics, Texas A&M University-Kingsville, 700 University Blvd., Kingsville, USA, 2020.

[20]. R. Adeoye, O. Adetan, O.D. Alowolodu - "Pythagorean Triple Based Cryptography System for Information Security", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 9, 2016.

[21]. Subhash Kak,- "Pythagorean Triples and Cryptographic Coding", Oklahoma State University, Stillwater. U.S.A. 2010.

[22]. Yegnanarayanan V., Poojitha Yakkala - "Pythagorean Triples in Cryptography and Associated Networks". International Journal of Innovative Technology and Exploring Engineering (IJITEE). Vol. 8, Issue 12, pg. 832-837. DOI: 10.35940/ijitee.L3221.1081219, 2019.