Qeios

Symmetric Key generation And Tree Construction in Cryptosystem based on Pythagorean and Reciprocal Pythagorean Triples

Dr T.SRINIVAS
Department of H&S, Professor, Priyadarshini College of Engineering &Technology, SPSR NELLORE, Andhra Pradesh, India.
E-mail id: srinivasthiruchinapalli@gmail.com

Abstract: Key generation and Secure are critical to the security of a Cryptosystem. Key generation and key exchange is the most challenging part of cryptography. In this paper, a scheme for symmetric key generation based on Pythagorean and Reciprocal Pythagorean triple has been presented. The proposed scheme incorporates a Key Distribution Centre (KDC) for user authentication and the secure exchange of secret information to generate keys. The KDC operation involves a request from a user for initiation. The KDC authenticates authenticate and secures the exchange of secret information to generate keys. The KDC authenticates the initiator. If the authentication is successful, KDC generates and sends an encrypted timestamp to both the initiator and responder. The proposed system is based on a novel mechanism to determine Pythagorean and Reciprocal Pythagorean triples to generate keys.

Introduction:

From the References [1],[2],[3],[4],[5],[6],[7],[8],[9],[10], Equations to be solved with integer values of the unknowns are now called Diophantine equations and the study of such equations is known as Diophantine Analysis. The equation $x^2 + y^2 = z^2$ for Pythagorean triples is an example of a Diophantine equation.

Euclid's formula is a fundamental formula for generating Pythagorean triples given a self-assertivematch of whole numbers m and n; with $m > n > 0$. The formula states that the integers

$a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$ form triple, Pythagorean.

By Euclid's formula triple is primitive if and only if m and n are coprime and not both odd. Whenboth m and n are odd, then a, b, and c will be even, and the triple will not be primitive.

The following will generate all Pythagorean triples remarkably:

$a = k \cdot (m^2 - n^2)$, $b = k \cdot (2mn)$, $c = k \cdot (m^2 + n^2)$

where m, n, and k are +ve integers with $m > n$, and with m and n odd, not both at the same time andcoprime. Since the time of Euclid, several formulas for generating triples with specific conditions have been established

https://doi.org/10.32388/MTTDWD

Various Methods to Generating Pythagorean Triple:
From References [10],[11],[12],[13],[14],[15],[16],[17],[18],[19],[20],[21],[22],[23],[24],[25],[26],[27] following results will be occurred

Case1: to Generate a Pythagorean Triple (x_1, x_2, x_3) for each x_1,there exists at least one x_2 and at least one x_3 , with $x_2 = \left|ax_1^2 - \frac{1}{4a}\right|$, $x_3 = \left|ax_1^2 + \frac{1}{4a}\right|$,

where $a = \left\{ \begin{matrix} \left\{\frac{1}{2p}, p \text{ is a factor of } x_1^2, if\ x_1 \text{ is an odd}\right. \\ \left\{\frac{1}{4p}, p \text{ is a factor of } \left(\frac{x_1}{2}\right)^2, if\ x_1 \text{ is an even}\right. \end{matrix} \right\}$

Case1.1: **If x_1 is an odd**

Consider $x_2 = \left|ax_1^2 - \frac{1}{4a}\right|$ since p is a factor of x_1^2.

Therefore $x_1^2 = np$ where n is an integer

$x_2 = \left|\frac{np}{2p} - \frac{1}{4\left(\frac{1}{2p}\right)}\right| = \left|\frac{n-p}{2}\right|$, both n and p odd numbers $\frac{n-p}{2}$ become an integer.

Similarly, $x_3 = \left|ax_1^2 + \frac{1}{4a}\right|$ since p is a factor of x_1^2. Therefore

$x_1^2 = np$ where n is an integer.

$x_3 = \left|\frac{np}{2p} + \frac{1}{4\left(\frac{1}{2p}\right)}\right| = \left|\frac{n+p}{2}\right|$, both n and p odd numbers $\frac{n+p}{2}$ become an integer.

Hence (x_1, x_2, x_3) becomes a Pythagorean Triple.

Table 1: Some results are represented below:

x_1	Choose p (Factor of x_1^2)	$n = \frac{x_1^2}{p}$	$x_2 = \left\|ax_1^2 - \frac{1}{4a}\right\| = \frac{n-p}{2}$	$x_3 = \left\|ax_1^2 + \frac{1}{4a}\right\| = \frac{n+p}{2}$	(x_1, x_2, x_3)
3	1	9	4	5	(3,4,5)
15	1	225	112	113	(15,112,113)
15	3	75	36	39	(15,36,39)

Computer programming (c #) to Generate Pythagorean Triples for x is an odd integer from 3 to 100 as follows

For x is an odd integer:

Program:

```
var output = new List<Tuple<int, int, int, int, int>>();
var facts = new Dictionary<int, List<int>>();
for (int i = 3; i <=100; i++)
{
    //  for x is odd integer
    if (i % 2 != 0)
    {
        facts.Add(i, Factor(i*i));
    }
}
for each (var item in facts)
{
    var x1= item.Key;
    for each (var item2 in item. Value)
    {
        var p = item2;
        var n = (x1 * x1) / p;
        var x2 = Math.Abs((n - p) / 2);
        var x3 = (n + p) / 2;
        output.Add(Tuple.Create(x1, p, n, x2, x3));
    }
}
Console.WriteLine($"| x1  |  p  |  n  |  x2  |  x3   |  (x1,x2,x3)  ");
Console.WriteLine();
for each (var item in output)
{
    Console.WriteLine($"|{item.Item1,5}|{item.Item2,5}|{item.Item3,5}| {item.Item4,5}| {item.Item5,5} |
{(item.Item1,item.Item4,item.Item5),5}  ");
}
List<int> Factor(int number)
{
    var factors = new List<int>();
    int max = (int)Math.Sqrt(number);  // Round down
    for (int factor = 1; factor <= max; ++factor) // Test from 1 to the square root, or the int below it, inclusive.
    {
        if (number % factor == 0)
        {
```

```
            factors.Add(factor);
            if (factor != number / factor) // Don't add the square root twice!
                factors.Add(number / factor);
        }
    }
    return factors;
}
```

Case 1.2: If x_1 is an even.

Consider $x_2 = \left|ax_1^2 - \frac{1}{4a}\right|$ since p is a factor of $\left(\frac{x_1}{2}\right)^2$. There fore

$$x_1^2 = 4np \text{ where } n \text{ is an integer}$$

$x_2 = \left|\frac{4np}{4p} - \frac{1}{4\left(\frac{1}{4p}\right)}\right| = |n - p|$, both n and p are integers, hence x_2 is also an integer.

Similarly, $x_3 = \left|ax_1^2 + \frac{1}{4a}\right|$ since p is a factor of$\left(\frac{x_1}{2}\right)^2$. Therefore

$x_1^2 = 4np$ where n is an integer

$x_3 = \left|\frac{np}{4p} + \frac{1}{4\left(\frac{1}{4p}\right)}\right| = |n + p|$, both n and p are integers, hence x_3 is also an integer.

Hence (x_1, x_2, x_3) becomes a Pythagorean Triple.

Table 2: Some results are represented below:

x_1	Choose p (Factor of $\left(\frac{x_1}{2}\right)^2$)	$n = \frac{x_1^2}{4p}$	$x_2 = \left\|ax_1^2 - \frac{1}{4a}\right\| = n - p$	$x_3 = \left\|ax_1^2 + \frac{1}{4a}\right\| = n + p$	(x_1, x_2, x_3)
4	1	4	3	5	(4,3,5)
6	3	3	0	6	(6,0,6)
6	1	9	8	10	(6,8,10)
8	1	16	15	17	(8,15,17)
8	2	8	6	10	(8,6,10)

Computer programming (c #) to Generate Pythagorean Triples for x is an even integer from 2 to 100 as follows

Program:

```
var output = new List<Tuple<int, int, int, int, int>>();
var facts = new Dictionary<int, List<int>>();
for (int i = 3; i <=100; i++)
```

```
{
   //  for x is Even integer
   if (i % 2 == 0)
   {
      facts.Add(i, Factor(((i/2) * (i/2)) ) );
   }
}
for each (var item in facts)
{
   var x1= item.Key;
   for each (var item2 in item. Value)
   {
      var p = item2;
      var n = (x1 * x1) / (4 *p);
      var x2 = Math.Abs(n - p) ;
      var x3 = (n + p);
      output.Add(Tuple.Create(x1, p, n, x2, x3));
   }
}
Console.WriteLine($"| x1  |  p  |  n  |  x2  |  x3   |  (x1,x2,x3)  ");
Console.WriteLine();
for each (var item in output)
{
   Console.WriteLine($"|{item.Item1,5}|{item.Item2,5}|{item.Item3,5}| {item.Item4,5}| {item.Item5,5} |
{(item.Item1,item.Item4,item.Item5),5}  ");
}
List<int> Factor(int number)
{
   var factors = new List<int>();
   int max = (int)Math.Sqrt(number);  // Round down
   for (int factor = 1; factor <= max; ++factor) // Test from 1 to the square root, or the int below it, inclusive.
   {
      if (number % factor == 0)
      {
         factors.Add(factor);
         if (factor != number / factor) // Don't add the square root twice!
            factors.Add(number / factor);
      }
   }
   return factors;
}
```

Case 1.3: Another Method to Generate Pythagorean Primitive Triple

Theorem: Choose a and b and $c^2 = 2\,a\,b$. Then $(a + c\,, b + c, a + b + c)$ is a Pythagorean Triple

Proof: Consider $(a + b + c)^2 - (a + c)^2 = (a + c)^2 + b^2 + 2(a + c)b - (a + c)^2$

$$= b^2 + 2(a + c)b \;= b^2 + 2ab + 2bc$$

But $c^2 = 2ab$ implies $2a = \frac{c^2}{b}$. imply $(a + b + c)^2 - (a + c)^2 = (\mathrm{b} + \mathrm{c})^2$.

Hence $(a + c, b + c, a + b + c)$ becomes a Pythagorean Triple when $c^2 = 2\,a\,b$.

Let a, and b are relatively prime then $(a + c, b + c, a + b + c)$ is a Primitive, otherwise, it becomes to Non-primitive Pythagorean Triple.

Table 3: Some results are represented below table:

A	b	$c= \sqrt{2ab}$	$x_1 = a + c$	$x_2 = b + c$	$x_3 = a + b + c$	(x_1, x_2, x_3)
2	9	6	8	15	17	(8,15,17)
2	4	4	6	8	10	(6,8,10)
3	6	6	9	12	15	(9,12,15)

Now we can go to introduce another Method to Generate Pythagorean Triple using Fibonacci and Pell numbers**.**

Case 1.4: Introduce Generate Pythagorean Triples using a sequence of **Fibonacci numbers** as follows. Let $\emptyset : \mathbf{Z^2} \rightarrow \mathbf{Z^3}(\boldsymbol{P})$ with

$$\boldsymbol{\emptyset(\mathrm{F_n}, \mathrm{F_{n+1}}) = ((2\mathrm{F_{n+1}}(\mathrm{F_n} + \mathrm{F_{n+1}})\,, \mathrm{F_n}(2\mathrm{F_{n+1}} + \mathrm{F_n}), \mathrm{F_{n+1}^2} + (\mathrm{F_n} + \mathrm{F_{n+1}})^2)}.$$

From Chapter 1, the sequence of Fibonacci numbers is $(\{\mathbf{1, 1, 2, 3, 5, 8, 13, 21} \dots\dots..\}$ following Recurrence Relation $\mathbf{F_n = F_{n-1} + F_{n-2}}$ **for** $\mathbf{n \geq 2}$, **with** $\mathbf{F_0 = 1, F_1 = 1}$.

Now we can go to study the generation of Pythagorean Triples using Fibonacci numbers as follows.

Table 4: Some results are represented below**:**

F_n	F_{n+1}	$(2(F_{n+1}(F_n + F_{n+1})\,, F_n(2F_{n+1} + F_n), F_{n+1}^2 + (F_n + F_{n+1})^2)$
1	1	(4,3,5)

1	2	(12,5,13)
2	3	(30,16,34)
3	5	(80,39,89)
5	8	(208,105,233)

Case 1.5: Introduce generating Pythagorean Triples using a sequence of **Pell numbers** as follows.

Let $\boldsymbol{\varphi}: \mathbf{Z}^2 \to \mathbf{Z}^3(\boldsymbol{P})$ with $\boldsymbol{\varphi}(\mathbf{P_n}, \mathbf{P_{n+1}}) = (2\boldsymbol{P_n P_{n+1}}, \boldsymbol{P_{n+1}^2} - \mathbf{P_n^2}, \mathbf{P_{n+1}^2} + \mathbf{P_n^2})$.

From Chapter 1, Pell Numbers$\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{5}, \mathbf{12}, \mathbf{29} \ldots \ldots, \}$ are Satisfies following Recurrence Relation $\boldsymbol{P_n = 2P_{n-1} + P_{n-2}}$ **for** $\boldsymbol{n \geq 2}$, **with** $\boldsymbol{P_0 = 0}$, $\boldsymbol{P_1 = 1}$. Now we can go to study the generation of Pythagorean Triples using pell numbers as follows.

Table 5: Some results are represented below:

P_n	P_{n+1}	$(2P_nP_{n+1}, P_{n+1}^2 - P_n^2, P_{n+1}^2 + P_n^2)$
0	1	(0,1,1)
1	2	(4,3,5)
2	5	(20,21,29)
5	12	(120,119,169)
12	29	(696,697,985)

Note: in a cryptographic system, symmetric key generation is depending on two consecutive Values of Fibonacci and Pell numbers**.**

Case 2: Generating Reciprocal Pythagorean Triples

The solutions of the Diophantine Equation $\mathbf{x^n + y^n = z^n}$ are satisfied the Reciprocal Pythagorean Theorem RPT = $\left\{(x, y, z) \in z^3: \frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}\right\}$ for $n = -2$.

The Reciprocal Pythagorean Theorem relates the two legs a, b to the altitude h is defined as follows $\frac{1}{a^2}+\frac{1}{b^2}=\frac{1}{h^2}$ with $c=\frac{ab}{h}$.

Now introduce a Method, to Generate a Set of Reciprocal Pythagorean Triples using Euclid's methodology of Generation of Pythagorean Triples.

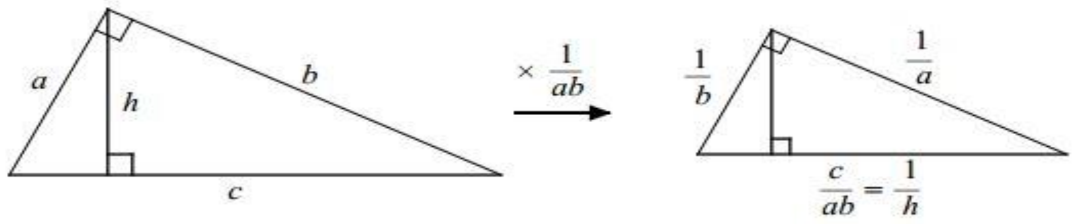


Figure 3: Reciprocal Pythagorean Theorem

Consider the Reciprocal Pythagorean Theorem $\frac{1}{x^2}+\frac{1}{y^2}=\frac{1}{z^2}$. It follows that $\frac{1}{x^2}=\frac{1}{z^2}-\frac{1}{y^2}$.

Again Simplify, $1=\frac{x^2}{z^2}-\frac{x^2}{y^2}$. It will follow that $\left(\frac{x}{z}+\frac{x}{y}\right)\left(\frac{x}{z}-\frac{x}{y}\right)=1$

The above equations must satisfy the following conditions for some positive integers p, q.

$$\frac{x}{z}+\frac{x}{y}=\frac{p}{q}, \quad \frac{x}{z}-\frac{x}{y}=\frac{q}{p}$$

From the above equations, $2x = z\left(\frac{p}{q}+\frac{q}{p}\right)$, $2x = y\left(\frac{p}{q}-\frac{q}{p}\right)$

Choose, two positive integers p, q ($p > q$), let x $= (p^2+q^2)(p^2-q^2)$.

It follows that $z = 2pq(p^2-q^2)$ and $y = 2pq(p^2+q^2)$

Consider $\frac{1}{x^2}+\frac{1}{y^2} = \frac{1}{((p^2+q^2)(p^2-q^2))^2}+\frac{1}{(2pq(p^2+q^2))^2} = \frac{1}{(2pq(p^2-q^2))^2} = \frac{1}{z^2}$

Table 6: Some results are represented below:

p	q	x	y	z	Reciprocal Pythagorean Triples
2	1	15	20	12	(15,20,12)
3	1	80	60	48	(80,60,48)
3	2	65	156	60	(65,156,60)

Computer programming to Generate a subset of the set of Reciprocal Pythagorean Triples

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

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
int main()
{
    int p, q;
    double x, y, z;
    for(p=2; p<=30;p++)
    {
        for(q=2;q<=30;q++)
            {
                if( p > q)
                {
                    x = ((pow(p,2) + pow(q,2)) * (pow(p,2) - pow(q,2)));
                    y = 2 * p * q * (pow(p,2) + pow(q,2));
                    z = 2 * p * q * (pow(p,2) - pow(q,2));
                    printf("For p= %d, q= %d; Values of (x,y,z) are (%.2f, %.2f, %.2f) \n", p, q, x, y,
z);
                }
            }
    }
    return 0;
}
```

If (x, y, z) is a Pythagorean triple then (y z, x z, x y) is a Reciprocal Pythagorean triple, (y z, x z, z^2) is a Pythagorean triple and vice versa. Extended this Lemma to generate at most all Pythagorean and Reciprocal Pythagorean n-tuples.

Corollary 2.1: Each Pythagorean Triple (x, y, z) is having corresponding Reciprocal Pythagorean Triple in the form of (xz, yz, xy).

Proof: Each Pythagorean Triple (x, y, z) is having corresponding Reciprocal Pythagorean Triple in the form of (xz, yz, xy) since $\frac{1}{(xz)^2} + \frac{1}{(yz)^2} = \frac{y^2+x^2}{(xyz)^2} = \frac{z^2}{(xyz)^2} = \frac{1}{(xy)^2}$.

From Case 2.2, If $\frac{a}{b} = x$, Now we can introduce to define some subsets of a Set of Reciprocal Pythagorean Triple as follows:

Table 7: $A' = \left\{(xz, yz, xy): \frac{z}{y} = 1 + \frac{2}{x^2-1} \text{ if } x \text{ is odd prime number or its power}\right\}$:

a	b	$x = \frac{a}{b}$	Corresponding Primitive Pythagorean Triples	Corresponding Reciprocal Pythagorean Triples
3	1	3	(3,4,5)	(15,20,12)
30	6	5	(5,12,13)	(65,156,60)
45	5	9	(9,40,41)	(369,1640,360)
100	4	25	(25,312,313)	(7825,97656,7800)
49	7	7	(7,24,25)	(175,600,168)

In this way, we can choose a, b values to obtain $\frac{a}{b} = x$ and apply the results of case 2.2 to generate Reciprocal Pythagorean Triples.

Table 8:

$$B' = \left\{ \begin{array}{c} (xz, yz, xy): \\ \frac{z}{y} = 1 + \frac{2}{\left(\frac{x}{(2p-1)^2}\right)^2 - 1} \text{ if } x \text{ is odd composite or its power and for some } p = 1,2,3\ldots \end{array} \right\}:$$

The odd composite number x	Pythagorean Primitive Triples	Corresponding Reciprocal Pythagorean Triples
15	(15,112,113), (15,8,17)	(1695,12656,1680), (255,136,120)
21	(21,220,221),(21,20,29)	(4641,48620,4620), (609,580,420)

33	(33,544,545),(33,56,65)	(17985,296480,17952), (2145,3640,1848)

Table 9: some results are represented in the below table if x is in 2 powers.

$$C' = \left\{ (xz, yz, xy) : \frac{z}{y} = 1 + \frac{2}{\left(\frac{x}{2}\right)^2 - 1} \text{ if } x \text{ is geometric power of } 2 \right\}:$$

Table 2.15:

x is the power of 2	Primitive Pythagorean Triples (For *p* = 1)	Corresponding Reciprocal Pythagorean Triples
4,8,16, 32...	(4,3,5), (8,15,17),(16,63,65),(32,255,257),…….	(20, 15, 12), (136, 255, 120), (1040, 4095, 1008),…

Table 10:

Some results of Pythagorean Triples for x are composite even numbers and $x > 2p^2$.

$$D' = \left\{ (xz, yz, xy) : \frac{z}{y} = 1 + \frac{2}{\left(\frac{x}{2p^2}\right)^2 - 1}, (x \text{ is an even composite number or its power}) \right\}:$$

Even a composite of *x*	primitive Triple	Nonprimitive Triple	Corresponding Reciprocal Pythagorean Triples
6	(3,4,5)	(6,8,10)	(15,20,12) (60,80,48)
10	(5,12,13)	(10,24,25)	(65,156,60), (250,600,240)
12	(12,35,37) , (12,5,13)	-	(444, 1295, 420), (156,65,60)
14	(7,24,25)	(14,48,50)	(175,600,168), (700,2400,720)
18	(9,40,41)	(18,80,82)	(369,1640,360), (1476,6560,1440)
20	(20,99,101),(20,21,29)	-	(2020,9999,1980), (580,609,420)

Case 2.6.1: Some Other method to Generate Reciprocal Pythagorean Triple

$$Rpt_o(x) = \left\{\left(\frac{x(x^2+1)}{2}, \frac{(x^2-1)(x^2+1)}{4}, \frac{x(x^2-1)}{2}\right) : x \text{ is an odd number greater than } 1\right\}$$

For generalization $Rpt_o(\boldsymbol{x}) = \left\{\left(\frac{(2m+1)((2m+1)^2+1)}{2}, \frac{((2m+1)^4-1)}{4}, \frac{(2m+1)((2m+1)^2-1)}{2}\right) : \boldsymbol{m} = \mathbf{1}, \mathbf{2}, \mathbf{3}, \dots\dots\right\}$

Table 11: Some results of $X_1 = \frac{x(x^2+1)}{2}$, $Y_1 = \frac{(x^2-1)(x^2+1)}{4}$, $Z_1 = \frac{x(x^2-1)}{2}$ are represented in below table:

m	x	X_1	Y_1	Z_1	Reciprocal Triple	(X_1, Y_1, Z_1)
1	3	15	20	12	(15,20,12)	(15,20,12)
2	5	65	156	60	(65, 156, 60)	(65, 156, 60)
3	7	175	600	168	(175, 600, 168)	(175, 600, 168)
4	9	369	1640	360	(369, 1640, 360)	(369, 1640, 360)
5	11	671	3660	660	(671, 3660, 660)	(671, 3660, 660)

Case 2.6.2: By choosing *x* is an even integer.

$$Rpt_e(x) = \left\{\left(x\left(\left(\frac{x}{2}\right)^2+1\right)\right), \left(\left(\frac{x}{2}\right)^2-1\right)\left(\left(\frac{x}{2}\right)^2+1\right), x\left(\left(\frac{x}{2}\right)^2-1\right) : x \text{ is an even number greater than } 2\right\}$$

For generalization,

$$Rpt_e(x) = \{(2m(m^2+1)), (m^4-1), 2m(m^2-1) : m = 2,3, \dots\dots\dots\}$$

Table 12: Some results of $X_1 = x\left(\left(\frac{x}{2}\right)^2+1\right), Y_1 = \left(\left(\frac{x}{2}\right)^2-1\right)\left(\left(\frac{x}{2}\right)^2+1\right), Z_1 = x\left(\left(\frac{x}{2}\right)^2-1\right)$ are represented in below table:

m	x	X_1	Y_1	Z_1	Reciprocal Triple	(X_1, Y_1, Z_1)
2	4	20	15	12	(20, 15, 12)	(20, 15, 12)
3	6	60	80	48	(60, 80, 48)	(60, 80, 48)
4	8	136	255	120	(136, 255, 120)	(136, 255, 120)

5	10	260	624	240	(260, 624, 240)	(260, 624, 240)
6	12	444	1295	420	(444, 1295, 420)	(444, 1295, 420)

Case 2.6.3: From case 2.3.3 and corollary 2.1, Reciprocal Pythagorean Triple is

$$\left(\boldsymbol{x_1}\left(\left|\boldsymbol{a x_1^2}+\frac{\mathbf{1}}{\mathbf{4a}}\right|\right),\left(\left|\boldsymbol{a x_1^2}-\frac{\mathbf{1}}{\mathbf{4a}}\right|\right)\left(\left|\boldsymbol{a x_1^2}+\frac{\mathbf{1}}{\mathbf{4a}}\right|\right),\boldsymbol{x_1}\left|\left(\boldsymbol{a x_1^2}+\frac{\mathbf{1}}{\mathbf{4a}}\right)\right|\right)$$

Table 13: Some examples are represented below table:

x_1	Triple(x_1, x_2, x_3)	Corresponding Reciprocal(x_1x_3, x_2x_3, x_1x_2)
3	(3,4,5)	(15,20,12)
4	(4,3,5)	(20,15,12)
6	(6,8,10)	(60,80,48)
8	(8,15,17)	(136,255,120)
12	(12,35,37)	(444,1295,420)
15	(15,36,39)	(585,1404,540)
15	(15,112,113)	(1695,12656,1680)
21	(21,28,35)	(735,980,588)
21	(21,72,75)	(1575,5400,1512)
21	(21,220,221)	(4641,48620,4620)

In this way, we can continue to generate Reciprocal Pythagorean Triples using of Fibonacci and Pell numbers by applying the results of Case 2.3.5 and Case 2.3.6,

Table 14: Using Fibonacci Numbers to Generate Reciprocal Triples:

F_n	F_{n+1}	Pythagorean Triple	Reciprocal Pythagorean Triple
1	1	(4,3,5)	(20,15,12)

1	2	(12,5,13)	(156,65,60)
2	3	(30,16,34)	(1020,544,480)
3	5	(80,39,89)	(7120,3471,3120)
5	8	(208,105,233)	(48464,24465,21840)

Table 15: Using Pell Numbers to Generate Reciprocal Triples:

P_n	P_{n+1}	Pythagorean Triple	Reciprocal Pythagorean Triple
0	1	(0,1,1)	(0,1,0), which is obviously True because of the value reaches to infinity
1	2	(4,3,5)	(20,15,12)
2	5	(20,21,29)	(580,609,420)
5	12	(120,119,169)	(20280,20111,14280)
12	29	(696,697,985)	(685560,686545,485112)

Lemma 2.1: If (x, y, z) is a Pythagorean triple then (y z, x z, x y) is a Reciprocal Pythagorean triple and vice versa.

Proof: Let (x, y, z) is a Pythagorean triple. i.e., $x^2 + y^2 = z^2$.

Consider $\frac{1}{(yz)^2} + \frac{1}{(xz)^2} = \frac{x^2+y^2}{x^2y^2z^2} = \frac{1}{(xy)^2}$. Hence (y z, x z, x y) is Reciprocal Pythagorean Triple. Successively applying the same operation we obtain (x^2yz, y^2xz, z^2xy) is a Pythagorean Triple. Since $(x^2yz)^2 + (y^2xz)^2 = (xyz)^2(x^2 + y^2) = (z^2xy)^2$.

Lemma 2.2: If (x, y, z) is a Pythagorean triple then then (y z, x z, z^2) is a Pythagorean triple.

Proof: Consider $(yz)^2 + (xz)^2 = z^2(x^2 + y^2) = z^4$. Hence (y z, x z, z^2) is a Pythagorean triple.

It follows that If (x, y, z) is a Pythagorean triple then (y z, x z, x y) is a Reciprocal Pythagorean triple and (y z, x z, z^2) is a Pythagorean triple. In this way, we can generate Pythagorean and Reciprocal Pythagorean triple with same two legs. Some results are represented in the below table

Table 16: Some Results of Pythagorean and Reciprocal Pythagorean triples with same two legs

Pythagorean Triple (x, y, z) $x^2+y^2=z^2$	(y z, x z, x y) is a Reciprocal Pythagorean triple $\frac{1}{(yz)^2}+\frac{1}{(xz)^2}=\frac{1}{(xy)^2}$	(y z, x z, z^2) is a Pythagorean triple $(yz)^2+(xz)^2=z^4$
(3,4,5)	(20,15,12)	(20,15,25)
(5,12,13)	(156,65,60)	(156,65,169)
(7,24,25)	(175,600,168)	(175,600,625)
(8,15,17)	(255,136,120)	(255,136,289)
(6,8,10)	(80,60,48)	(80,60,100)
(9,40,41)	(1640,369,360)	(1640,369,1681)
(10,24,26)	(624,260,240)	(624,260,676)

Corollary1: Now we can apply Lemma 1 to generate successively alternate Pythagorean and Reciprocal Pythagorean triples respectively

Table 17: Generating of Pythagorean and Reciprocal Pythagorean triples using Lemma 1

Pythagorean Triples	Reciprocal Pythagorean Triples
(x,y,z)	(yz,xz,xy)
(x^2yz,y^2xz,z^2xy)	$(x^2y^3z^3,y^2x^3z^3,z^2x^3y^3)$
$(x^6y^5z^5,y^6x^5z^5,z^6x^5y^5)$ [Since $(x^6y^5z^5)^2+(y^6x^5z^5)^2$ $=(y^5x^5z^5)^2(x^2+y^2)$ $=(z^6x^5y^5)^2$].	$(x^{10}y^{11}z^{11},y^{10}x^{11}z^{11},z^{10}x^{11}y^{11})$ [since $\frac{1}{(x^{10}y^{11}z^{11})^2}+\frac{1}{(y^{10}x^{11}z^{11})^2}$ $=\frac{1}{(x^{10}y^{10}z^{10})^2}\left[\frac{1}{(yz)^2}+\frac{1}{(xz)^2}\right]$ $=\frac{1}{(x^2y^2z^2)^2}\frac{1}{(xy)^2}=\frac{1}{(z^2x^3y^3)^2}$]

$(x^{22}y^{21}z^{21}, y^{22}x^{21}z^{21}, z^{22}x^{21}y^{21})$ [since $(x^{22}y^{21}z^{21})^2 + (y^{22}x^{21}z^{21})^2$ $= (x^{21}y^{21}z^{21})^2\,(x^2+y^2) = (z^{22}x^{21}y^{21})^2$	$(x^{42}y^{43}z^{43}, y^{42}x^{43}z^{43}, z^{42}x^{43}y^{43})$ [since $\frac{1}{(x^{42}y^{43}z^{43})^2} + \frac{1}{(y^{42}x^{43}z^{43})^2}$ $= \frac{1}{(x^{42}y^{42}z^{42})^2}\left[\frac{1}{(yz)^2} + \frac{1}{(xz)^2}\right]$ $= \frac{1}{(x^{42}y^{42}z^{42})^2}\frac{1}{(xy)^2} = \frac{1}{(z^{42}x^{43}y^{43})^2}$]
$(x^{86}y^{85}z^{85}, y^{86}x^{85}z^{85}, z^{86}x^{85}y^{85})$ [since $(x^{86}y^{85}z^{85})^2 + (y^{86}x^{85}z^{85})^2$ $= (x^{85}y^{85}z^{85})^2\,(x^2+y^2) = (z^{86}x^{85}y^{85})^2$]	$(x^{170}y^{171}z^{171}, y^{170}x^{171}z^{171}, z^{170}x^{171}y^{171})$ [since $\frac{1}{(x^{170}y^{171}z^{171})^2} + \frac{1}{(y^{170}x^{171}z^{171})^2}$ $= \frac{1}{(x^{170}y^{170}z^{170})^2}\left[\frac{1}{(yz)^2} + \frac{1}{(xz)^2}\right]$ $= \frac{1}{(x^{170}y^{170}z^{170})^2}\frac{1}{(xy)^2} = \frac{1}{(z^{170}x^{171}y^{171})^2}$]

Table 18: Some Results of Lemma 1, By choosing the initial Pythagorean triple (3,4,5)

Pythagorean Triples	Reciprocal Pythagorean Triples
(3,4,5)	(15,20,12)
(180,240,300)	(54000,72000,43200)
(2332800000,3110400000,3888000000)	$\left(\begin{matrix}9.0699264 * 10^{18}, 1.20932352 * 10^{19}, \\ 7.25594112 * 10^{18}\end{matrix}\right)$

Corollary 2: Now we can apply Lemma 1 to generate successively Pythagorean and Reciprocal Pythagorean triples respectively, where the initial Pythagorean triple is (x, y, z)

Table 19: Generating of Pythagorean and Reciprocal Pythagorean triples using Lemma 1

Pythagorean Triples	Reciprocal Pythagorean Triples
(yz, xz, z^2) $[since\ (yz)^2 + (xz)^2 = z^2(x^2+y^2) = z^4]$	(xz^3, yz^3, xyz^2) [since $\frac{1}{(xz^3)^2} + \frac{1}{(yz^3)^2}$ $= \frac{1}{(z^3)^2}\left[\frac{1}{x^2} + \frac{1}{y^2}\right] = \frac{1}{(xyz^2)^2}$
$(xy^2z^5, yx^2z^5, xyz^6)$ [since$(xy^2z^5)^2 + (yx^2z^5)^2$	$(x^3y^2z^{11}, y^3x^2z^{11}, x^3y^3z^{10})$

$= (xyz^5)^2(y^2 + x^2)$ $= (xyz^6)^2]$	[since $\frac{1}{(x^3y^2z^{11})^2} + \frac{1}{(y^3x^2z^{11})^2}$ $= \frac{1}{(x^2y^2z^{11})^2}\left[\frac{1}{x^2} + \frac{1}{y^2}\right]$ $= \frac{1}{(x^3y^3z^{10})^2}]$
$(x^5y^6z^{21}, y^5x^6z^{21}, x^5y^5z^{22})$ [since$(x^5y^6z^{21})^2 + (y^5x^6z^{21})^2 =$ $(x^5y^5z^{21})^2(y^2 + x^2)$ $= (x^5y^5z^{22})^2]$	$(x^{11}y^{10}z^{43}, y^{11}x^{10}z^{43}, x^{11}y^{11}z^{42})$ [since $\frac{1}{(x^{11}y^{10}z^{43})^2} + \frac{1}{(y^{11}x^{10}z^{43})^2}$ $= \frac{1}{(x^{10}y^{10}z^{43})^2}\left[\frac{1}{x^2} + \frac{1}{y^2}\right]$ $= \frac{1}{(x^{11}y^{11}z^{42})^2}]$

Table 20: Some Results of Lemma 1, By choosing the initial Pythagorean triple (3,4,5)

Pythagorean Triples	Reciprocal Pythagorean Triples
(20,15,25)	(500,375,300)

Case 3: Construction of Pythagorean and Reciprocal Pythagorean triple for 4-tuple

Lemma 3.1: If (a, b, c, d) is a Pythagorean 4-tuple $(a^2 + b^2 + c^2 = d^2)$ then (bcd, acd, abd, abc) becomes to corresponding Reciprocal Pythagorean 4-tuple.

Proof: Consider $\frac{1}{(bcd)^2} + \frac{1}{(acd)^2} + \frac{1}{(abd)^2} = \frac{a^2+b^2+c^2}{a^2b^2c^2d^2} = \frac{1}{(abc)^2}$. Hence (bcd, acd, abd, abc) is a Reciprocal Pythagorean 4-tuple. Continuing Lemma2 to above 4-tuple, we obtain successively Pythagorean and Reciprocal Pythagorean 4-tuples respectively.

Table 21: Generating of Pythagorean and Reciprocal Pythagorean 4-tuples using Lemma 2

Pythagorean 4-tuples	Reciprocal Pythagorean 4-tuples
(a, b, c, d)	(bcd, acd, abd, abc)
$(a^3b^2c^2d^2, b^3a^2c^2d^2, c^3a^2b^2d^2, d^3a^2b^2c^2)$	$\begin{pmatrix} a^6b^7c^7d^7, b^6a^7c^7d^7 \\ , c^6a^7b^7d^7, d^6a^7b^7c^7 \end{pmatrix}$
$(a^{21}b^{20}c^{20}d^{20}, b^{21}a^{20}c^{20}d^{20}, c^{21}a^{20}b^{20}d^{20}, d^{21}a^{20}b^{20}c^{20})$	$\begin{pmatrix} a^{60}b^{61}c^{61}d^{61}, b^{60}a^{61}c^{61}d^{61}, \\ c^{60}a^{61}b^{61}d^{61}, d^{60}a^{61}b^{61}c^{61} \end{pmatrix}$

Table 22: Some Results of Lemma 2.1, By choosing initial Pythagorean 4-tuple (3,4,12,13)

Pythagorean 4-tuple	Reciprocal Pythagorean 4-tuple
$(3,4,12,13)$	$(624,468,156,144)$
$(10513152,14017536,42052608,45556992)$	$\begin{pmatrix} 2.685465987 * 10^{22}, 2.01409949 * 10^{22}, \\ 6.713664967 * 10^{21}, 6.1972292 * 10^{21} \end{pmatrix}$

Note: If (a,b,c,d) is a Pythagorean 4-tuple $(a^2+b^2+c^2=d^2)$ then $\left(bc,ac,ab,\frac{abc}{d}\right)$ is identical form of Lemma 2. But it will not become a Reciprocal Pythagorean 4-tuple. We can verify this by taking one example.

Proof: Consider $\frac{1}{(bc)^2}+\frac{1}{(ac)^2}+\frac{1}{(ab)^2}=\frac{a^2+b^2+c^2}{a^2b^2c^2}=\frac{d^2}{(abc)^2}=\frac{1}{\left(\frac{abc}{d}\right)^2}$.

Hence $\left(bc,ac,ab,\frac{abc}{d}\right)$ is a Reciprocal Pythagorean 4-tuple.

Continuing Lemma 2.2 to above 4-tuple, we obtain successively Pythagorean and Reciprocal Pythagorean 4-tuples respectively.

Now we can choose Pythagorean 4 – tuple (3,4,12,13). Apply the above sufficient condition of $\left(bc,ac,ab,\frac{abc}{d}\right)$, which implies (48,36,12,144/13) is not a Reciprocal 4-tuple.

Case4: Construction of Pythagorean triple and Reciprocal Pythagorean for 5-tuple

Lemma 4.1: If (a,b,c,d,e) is a Pythagorean 5-tuple $(a^2+b^2+c^2+d^2=e^2)$ then $(bcde,acde,abde,abce,abcd)$ is becomes to corresponding Reciprocal Pythagorean 5-tuple.

Proof: Consider $\frac{1}{(bcde)^2}+\frac{1}{(acde)^2}+\frac{1}{(abde)^2}+\frac{1}{(abce)^2}=\frac{a^2+b^2+c^2+d^2}{a^2b^2c^2d^2e^2}=\frac{1}{(abcd)^2}$.

Hence $(bcde,acde,abde,abce,abcd)$ is a Reciprocal Pythagorean 5-tuple. Continuing Lemma3 to above 5-tuple, we obtain successively Pythagorean and Reciprocal Pythagorean 5-tuples respectively.

Table 23: Generating of Pythagorean and Reciprocal Pythagorean 5-tuples using Lemma 3

Pythagorean 5-tuples	Reciprocal Pythagorean 5-tuples
(a,b,c,d,e)	$(bcde,acde,abde,abce,abcd)$
$\begin{pmatrix} a^4b^3c^3d^3e^3, b^4a^3c^3d^3e^3, \\ c^4a^3b^3d^3e^3, d^4a^3b^3c^3e^3, e^4a^3b^3c^3d^3 \end{pmatrix}$	$\begin{pmatrix} a^{12}b^{13}c^{13}d^{13}e^{13}, b^{12}a^{13}c^{13}d^{13}e^{13}, \\ c^{12}a^{13}b^{13}d^{13}e^{13}, d^{12}a^{13}b^{13}c^{13}e^{13} \\ , e^{12}a^{13}b^{13}c^{13}d^{13} \end{pmatrix}$

Table 15: Some Results of Lemma 3, By choosing initial Pythagorean 5-tuple (3,4,12,84,85)

Pythagorean 5-tuple	Reciprocal Pythagorean 5-tuple

(3,4,12,84,85)	(342720,257040,85680,12240,12096)

Main Work:

In the proposed system, three parties are involved in the key exchange process. i.e

Key distribution center (KDC), source (A) and destination (B). If A wants to communicate with B using symmetric key encryption, a session must be created between them. A secret session key shared between and B is required for the encryption of data in this session

Application of Pythagorean Triple in Cryptosystem

Key generation and Secure are critical to the security of a Cryptosystem. If fact key generation and key exchange is the most challenging part of cryptography. In this chapter, a scheme for symmetric key generation based on the Pythagorean triple has been presented. The proposed scheme incorporates a Key Distribution Centre (KDC) for user authentication and secure exchange of secret information to generate keys. The KDC operation involves a request from a user for initiation. The KDC authenticates authenticate and secures the exchange of secret information to generate keys. The KDC authenticates the initiator. If the authentication is successful, KDC generates and sends an encrypted timestamp to both the initiator and responder.

The proposed system is based on a novel mechanism to determine Pythagorean triples to generate keys. The formula uses factors of x to generate y and z such that x, y, and z satisfy the Pythagorean theorem.

The following notation has been used for Pythagorean triple calculation

x- input to calculate Pythagorean triple

p_1 - First prime factor of x, p_2 - Second Prime factor of x

y and z – Key Pair, Suppose, If x is odd then y = $\frac{|x^2-p_1^2|}{2p_1}$ and z= $\frac{|x^2+p_1^2|}{2p_1}$ the final key is computed by XORing y and z. i.e. p = y ⊕ z

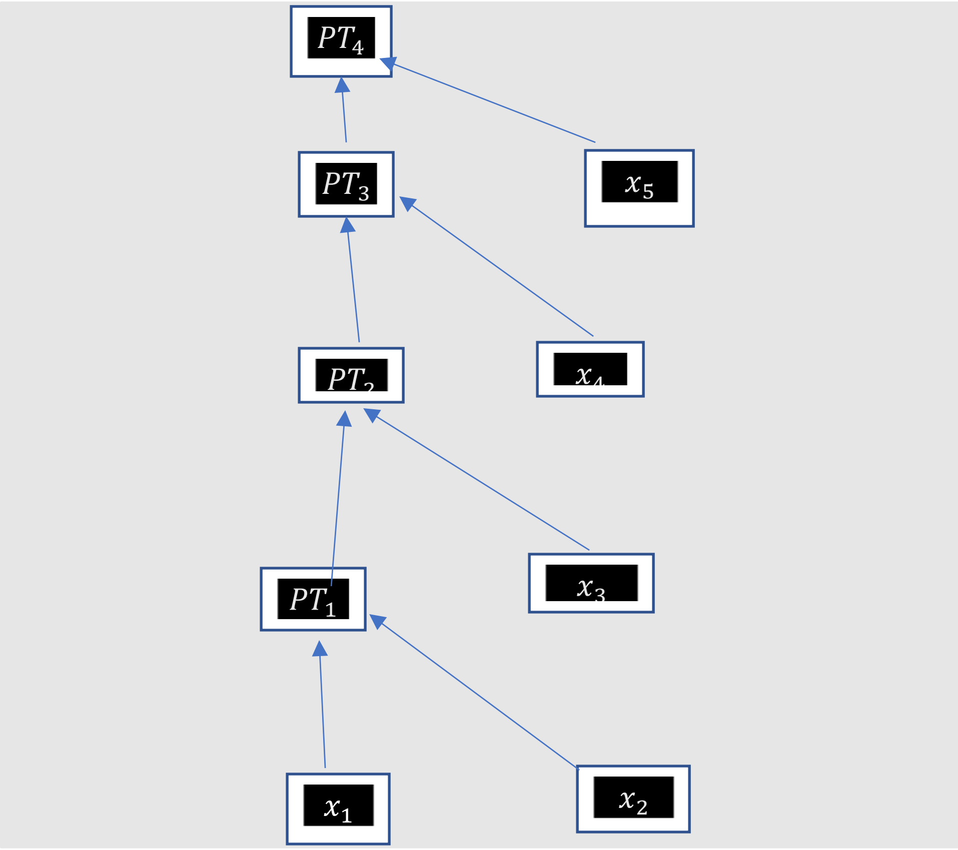
In the proposed system, three parties are involved in the key exchange process. i.e

Key distribution center (KDC), source (A) and destination (B). If A wants to communicate with B using symmetric key encryption, a session must be created between them. A secret session key shared between and B is required for the encryption of data in this session.

Construction of Pythagorean triple for n-tuple:

The Pythagorean n-tuple, $x_1^2 + x_2^2 + x_3^2 + x_4^2 + \cdots .. + x_{n-1}^2 = x_n^2$ has been used to construct a tree. A binary tree of height n has been generated whose leaf nodes are $x_i's$, for 1≤ I $\leq n-1$ and the root is x_n. As illustrated in the given Figure, the leaf nodes are [

$x_1, x_2, x_3, \dots \dots . x_i, \dots . . x_{n-1}]$ and the root is x_n which constitutes the Pythagorean n-tuples $[x_1, x_2, x_3, \dots \dots . x_i, \dots . . x_{n-1}, x_n]$ and satisfies the equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 + \cdots .. + x_{n-1}^2 = x_n^2$.



The Procedure is defined as follows:

Step 1: choose x_1 , where $x_1 > 3$;

Step 2: let t be a temporary variable initialized as follows;

t = x_1

Construct a binary tree (T) by taking t as the root, x_1 as the left child and x_2 as the right child which is calculated by applying step 3.

Step 3: for $1 \leq i \leq n-1$, apply the generation of key elements from the above methods.

For suppose, $x_{i+1} = a(t)^2 - \frac{1}{4a}$

$p_i = a(t)^2 + \frac{1}{4a}$,where **a** = $\left\{ \begin{array}{c} \left\{ \frac{1}{2p}, p \text{ is a factor of } x_1^2, \text{if } x_1 \text{ is odd} \right. \\ \left\{ \frac{1}{4p}, p \text{ is a factor of } \left(\frac{x_1}{2}\right)^2, \text{if } x_1 \text{ is even} \right. \end{array} \right\}$

t = p_i

apply the above algorithm to construct the Pythagorean tree.

Some integer sequences are satisfied with the properties given below.

$$3^2 + 4^2 = 5^2$$

$$3^2+4^2+12^2=13^2$$
$$3^2+4^2+12^2+84^2=\ 85^2$$
$$3^2+4^2+12^2+84^2+204^2=\ 221^2$$
$$3^2+4^2+12^2+84^2+720^2=725^2$$
$$3^2+4^2+12^2+84^2+204^2+60^2=\ 229^2$$
$$3^2+4^2+12^2+84^2+204^2+1428^2=\ 1445^2$$
$$3^2+4^2+12^2+84^2+720^2+1740^2=1885^2,$$
$$3^2+4^2+12^2+84^2+204^2+1872^2=\ 1885^2$$
$$3^2+4^2+12^2+84^2+720^2+2040^2=\ 2165^2$$

Conclusion:

The proposed system is based on a novel mechanism to determine Pythagorean triples to generate keys. The formula uses factors of x to generate y and z such that x, y, and z satisfy the Pythagorean theorem.

The following notation has been used for Pythagorean triple calculation

x- input to calculate Pythagorean triple

p_1 - First prime factor of x

p_2 - Second Prime factor of x

y and z – Key Pair

Suppose, If x is odd then y = $\frac{|x^2-p_1^2|}{2p_1}$ and z= $\frac{|x^2+p_1^2|}{2p_1}$ the final key is computed by XORing y and z.

i.e. p = y ⊕ z

In the proposed system, three parties are involved in the key exchange process. i.e

Key distribution center (KDC), source (A) and destination (B). If A wants to communicate with B using symmetric key encryption, a session must be created between them. A secret session key shared between and B is required for the encryption of data in this session.

References:

[1] **https://mathworld.wolfrom.com/pythagorean triples**

[2] A new approach to generate all Pythagorean triples by Anthony Overmars, AIMS Mathematics, 4(2):242-253.

[3] A textbook “Introduction to Analytic Number Theory “by Tom M. Apostol, Springer.

[4] Pythagorean Triples- www.mathsisfun.com

[5] L.E. Dickson., 2005 History of the theory of numbers: Diophantine analysis, Dover publications,

[6] A Hattangadi Exploration in Mathematics, 3rd Edition India: University Press,2008

[7] A.K.Hazra Matrix: Algebra, Calculus and Generalised Inverse 2010

[8] Bhupendra Singh Advanced Abstract Algebra 2002

[9] David M. Burton Elementary Number Theory, 2003

[10].Sridevi, K., & **Srinivas, T.** (2023). Transcendental representation of the Diophantine equation and some of its inherent properties. *Materials Today: Proceedings*, *80*, 1822-1825.

[11]. Sridevi, K., & **Srinivas, T.** (2023). Existence Of Inner Addition and Inner Multiplication On Set of Triangular Numbers and Some Inherent Properties of Triangular Numbers. *Materials Today: Proceedings*, *80*, 1822-1825.

[12].Sridevi, K., & **Srinivas, T.** (2023). Cryptographic coding To Define Binary Operation on a Set of Pythagorean Triples. *Materials Today: Proceedings*, *80*, 1822-1825

[13]. Srinivas, T., & Sridevi, K. (2022). Transcendental representation of Diophantine Equation $x^n + y^n = z^n$ to Generate At Most All Pythagorean and Reciprocal Pythagorean Triples. *JOURNAL OF ALGEBRAIC STATISTICS*, *13*(2), 3600-3609.

[14].Sridevi, K., & **Srinivas, T**. (2022). Algebraic Structure Of Reciprocal Pythagorean Triples. Advances And Applications In Mathematical Sciences, Volume 21, Issue 3, January 2022, P.1315-1327© 2022 Mili Publications, India Issn 0974-6803)

[15].**Srinivas, T**., & Sridevi, K. (2022, January). A new approach to define a new integer sequence of Fibonacci-type numbers using third-order linear Recurrence relations. In *AIP Conference Proceedings* (Vol. 2385, No. 1, p. 130005). AIP Publishing LLC

[16].**Srinivas, T**., & Sridevi, K. (2021, November). A New Approach to Define Algebraic Structure and Some Homomorphism Functions on Set of Pythagorean Triples and Set of Reciprocal Pythagorean Triples " in JSR (Journal of Scientific Research) (UGC CARE 1, Print Journal), Volume 65, Issue 9, November 2021, Pages 86-92.

[17].Sridevi, K., & Srinivas, T. (2020). A new approach to defining two types of binary operations on the set of Pythagorean triples to form as at most commutative cyclic semigroup. *Journal of Critical Reviews*, *7*(19), 9871-9878.

[18].SRINIVAS. T. (2020). Proof Of Fermat's Last Theorem By Choosing Two Unknowns in the Integer Solution Are Prime Exponents. *pacific international Journal*, *3*(4), 147-151. ISSN 2616-4825 [Online] 2663-8991 [Print] Volume number 03, issue number 03

[19].Srinivas, T. (2014). Transportation and its health implications in India. *Int. J. Eng. Res. Dev*, *10*(7), 67-73.

[20].Baggidi, P. R., Prasad, D. G., & **Srinivas, T**. (2013). Security enhancement in mobile ad hoc networks using non-zero noncooperative game theory. *International Journal of Research in Computer and Communication Technology*, *2*(8), 614-621.

[21].Srinivas, T., & Bathul) S,(2013). Monotonicity, IJSR (Issn:2277-8179)

[22].Srinivas, T., & Bathul S,(2013). Approximate Derivatives, IJSR (Issn:2277-8179)

[23].Srinivas, T., & Devi(2016) P. S. The Conventional Method of Optimizing Delivery Routes And Schedules.IJRCCT(2320-5156)

[24].Srinivas, T., & Devi,(2017) P. S Effective Ness And Illustration Of Distribution Systems And Supply Chain Management.IJECS(Issn:2319-7242))

[25].Srinivas T(2018), Taguchi Philosophy of Engineering Quality" in Pacific International Journal, ISSN 2616-4825 [Online] 2663-8991 [Print] Volume number 03, issue number 03

[26].Srinivas T(2018), Financial Soundness Of Selected Indian Petroleum Companies Using Altman Z–Score Model in Pacific International Journal, ISSN 2616-4825 [Online] 2663-8991 [Print] Volume number 03, issue number 03

[27]. Srinivas, T. (2023). Some Inherent Properties of Pythagorean Triples. *Research Highlights in Mathematics and Computer Science Vol. 7*, 156-169.