International Journal of Scientific Research in Mathematical and Statistical Sciences **Research Paper**
Vol.6, Issue.3, pp.115-120, June (2019) **E-ISSN:** 2348-4519
DOI: https://doi.org/10.26438/ijsrmss/v6i3.115120

Encryption with Key stream via Short vectors

P. Anuradha Kameswari [1*], S B T Sundari Katakam[2]

[1,2] Department of Mathematics, Andhra University,Visakhapatnam - 530003, Andhra Pradesh, India.

[*]*Corresponding Author: panuradhakameswari@yahoo.in Tel.: +91-9866815530*

Available online at: www.isroset.org

Received: 17/May/2019, Accepted: 10/Jun/2019, Online: 30/Jun/2019

***Abstract*—**In this paper we describe a cryptosystem with keystream for Encryption, based on concatenation of short vectors of lattices corresponding to quadratic forms, that are good rational approximations of $\sqrt{z}$, for z a non-perfect square number. This cryptosystem is employed by both Symmetric key and Public key cryptosystem that is based on the hard mathematical problem of retrieving an irrational number from the convergents obtained as short vectors.

Keywords*—*Encryption, key stream, short vector, LLL algorithm, Lattice reduction, quadratic form.

I. INTRODUCTION

There are basically two types of cryptosystems, namely Symmetric Key Cryptosystem(SKC) and Public Key cryptosystem(PKC). In SKC, same key is used for enciphering and deciphering or the deciphering key may be easily obtained by the knowledge of enciphering key. The main disadvantage of SKC is maintaining the secrecy of the key. To avoid this, PKCs have been introduced in which enciphering key and deciphering keys are different. But the main drawback of PKC is that it is not efficient enough in sending huge messages. These drawbacks have been settled by employing both SKC and PKC in a cryptosystem. PKC is adapted for key exchange and SKC is used to encode huge messages. Thus, strong and efficient cryptosystems can be build to send huge message with secrecy by employing both SKC and PKC.

The infinite decimal expansion structure of the irrational numbers plays a vital role in mathematics especially in cryptogaphy. Due to its infinite expansion one can find infinite rational approximations to the irrational. In [10] the stream ciphers based on the hard mathematical problem of retrieving an irrational number from its continued fraction expansion, the key streams are developed by concatenation of quotients of continued fraction expansion. In this paper we replace the role of quotients, by short vectors of lattices corresponding to quadratic forms and construct key streams for a cryptosystem.

In this paper in section II, we give some preliminaries on lattice reduction [7][13] and in section III we describe encryption with key stream via short vectors and describe efficiency in section IV and describe cryptanalysis in section V and we conclude in section VI.

II. PRELIMINARIES

Definition 1 A Lattice L is a discrete additive subgroup of $\mathbf{R}^m$, that is L is the $\mathbf{Z}$ −span of a linearly independent subset of $\mathbf{R}^m$:

$$L = \mathbf{Z}b_1 + \mathbf{Z}b_2 + \cdots + \mathbf{Z}b_n$$

with the quadratic form $q(x) =< x, x >$, for $x \in L$. The vectors $b_1, b_2, \ldots, b_n$ are a basis for L, and $A = [< b_i, b_j >]_{1 \le i,j \le n}$ is the corresponding Gram matrix also note $q(x) = x^T Ax$.

Definition 2 The short vector in a lattice L is a nonzero vector $v \in L$ that minimizes the Euclidean norm $||v||$. The problem of finding the vector $v \in L$ that minimizes $||v||$ is called the short vector problem denoted as SVP.

Definition 3 Let $\mathbf{B} = \{b_1, b_2, \ldots, b_n\}$ be a basis for a lattice L and let $\mathbf{B}^* = \{b_1^*, b_2^*, \ldots, b_n^*\}$ be the associated Gram - Schmidt orthogonal basis. The basis $\mathbf{B}$ is said to be *LLL* reduced if it satisfies the following two conditions:

1. $|\mu_{i,j}| = \frac{|b_i \cdot b_j^*|}{||b_j^*||^2} \le \frac{1}{2}$ for all $1 \le j < i \le n$.
2. $||b_i^*||^2 \ge (\frac{3}{4} - \mu_{i,i-1}^2)||b_{i-1}^*||^2$ for all $1 < i \le n$.

Theorem 1 Let L be a lattice of dimension n. Any *LLL* reduced basis $\{b_1', b_2', \ldots, b_n'\}$ for L has the following two properties:

1. $\prod_{i=1}^{n} ||b_{i'}|| \le 2^{n(n-1)/4} \det L$
2. $||b_j'|| \le 2^{(i-1)/2}||b_i^*||$ for all $1 \le j \le i \le n$.

Remark 1 An algorithm that returns an *LLL* reduced basis called *LLL* algorithm comes close to solve *SVP* in small dimensions, as the initial vector in an *LLL* reduced basis satisfies $||b_1'|| \leq 2^{n(n-1)/4}|\det L|^{1/n}$.

Remark 2 For any short vector $(x_1, x_2, \ldots, x_n)$ we have $q(x_1, \ldots x_n) \leq 2^{\frac{n-1}{2}} \det q^{\frac{1}{n}}$ [13].

Let α be a real number, then using the above remark 2 for $n = 2$, in the following theorem the short vector (x, y) of some $q(x, y)$ is interpreted as a rational approximation $\frac{y}{x}$ to α.

Theorem 2 [13] If α is a real number then for $M = 10^s$, for some $s > 0$,integer with $\bar{\alpha}$ a decimal approximation of α to precision $\frac{1}{M}$, any short vector (x, y) of the quadratic form $q(x, y) = M(\bar{\alpha}x - y)^2 + \frac{1}{M}x^2$ is such that $\frac{y}{x}$ is a rational approximation of α.

Proof. For a given α choose M with $\bar{\alpha}$, a decimal approximation to $\frac{1}{M}$ and the quadratic form $q(x, y) = M(\bar{\alpha}x - y)^2 + \frac{1}{M}y^2$. Now, we obtain the short vector (x, y) by reducing the lattice Z^2 equipped with quadratic form,

$$q(x, y) = M(\bar{\alpha}x - y)^2 + \frac{1}{M}x^2$$

The 2-dimensional Gram-matrix associated with the quadratic form is given by a symmetric positive definite matrix,

$$A = \begin{bmatrix} \bar{\alpha}^2 M + \frac{1}{M} & -\bar{\alpha}M \\ -\bar{\alpha}M & M \end{bmatrix}$$

whose determinant is 1, and hence it corresponds to a lattice of determinant 1 .

The underlying lattice in the Euclidean space R^2 is given by the matrix B,

$$B = \begin{bmatrix} \frac{1}{\sqrt{M}} & 0 \\ \bar{\alpha}\sqrt{M} & -\sqrt{M} \end{bmatrix}$$

whose columns forms a basis for the lattice. Let $b_i's$ be the rows of B^T. Applying LLL algorithm to B^T, the resultant of LLL is then a reduced basis B' of the same lattice. As B and B'^T are the matrices whose columns represent basis of the same lattice, B and B' are related by integer unimodular transformation matrix, U as $BU = B'^T$. Therefore, the matrix U, is obtained by $U = B^{-1}B'^T$

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

And the vector (a, c) is short vector (x, y). This short vector (x, y) is such that $\frac{x}{y}$ is a rational approximation of α.

By LLL for any short vector $(x_1, x_2, \ldots, x_n)$ we have $q(x_1, \ldots x_n) \leq 2^{\frac{n-1}{2}} \det q^{\frac{1}{n}}$, Thus, we have for the 2-dimensional lattice L above $q(x, y) \leq \sqrt{2}$.

Therefore, we have $|\bar{\alpha}x - y|^2 \leq \frac{\sqrt{2}}{M}$ and $|x|^2 \leq \sqrt{2}M$.

Now, as $\bar{\alpha}$ is a decimal approximation of α to precision $\frac{1}{M}$, we have $|\alpha - \bar{\alpha}| \leq \frac{1}{M}$ and using the inequalities above, we have $|\alpha x - y| = 2^{\frac{5}{4}}.\frac{1}{\sqrt{M}}$, which implies,

$$|\alpha - \frac{y}{x}| = |\frac{\alpha x - y}{x}| \leq \frac{2^{\frac{5}{4}}}{\sqrt{M}x} \leq \frac{2^{\frac{3}{2}}}{x^2} = \frac{1}{kx^2}, \quad \text{for} \quad k = \frac{1}{2^{\frac{3}{2}}}.$$

Therefore,as for all $k < \sqrt{5}$ by [6] we have $\frac{y}{x}$ is a rational approximation of α.

In the following section we generate key stream for encryption using short vectors.

III. ENCRYPTION WITH KEY STREAM VIA SHORT VECTORS

In the proposed encryption scheme first a common secret key z called key exchange is generated by using RSA and then a common key stream is developed using concatenation of short vector.

Key stream via short vectors:

For a given non-perfect square number z, a sequence of rational approximations of $\sqrt{z}$ may be obtained as short vectors of lattices corresponding to quadratic form

$$q(x, y) = M\left(\overline{\sqrt{z}}x - y\right)^2 + \frac{1}{M}x^2$$

for $M = 10^s, s \in \mathbb{N}$, and $\overline{\sqrt{z}}$ is decimal expansion of $\sqrt{z}$ corrected to s decimals. Thus, varying s from 1 onwards, we get a sequence of short vectors that are convergents and rational approximations of $\sqrt{z}$. Therefore, as the decimal expansion of $\sqrt{z}$, z a non-perfect square number, is infinite, we get inifinite sequence of short vectors. In this paper we employ these infinite sequence of short vectors in generating key streams for a cyptosystem.

Let s, r and $s < r$ be two fixed positive integers and let (p_i, q_i) be the short vectors of quadratic form

$$q(x,y) = M\left(\overline{\sqrt{z}}x - y\right)^2 + \frac{1}{M}x^2,$$

corresponding to $M = 10^i$, for all $i \ni s \le i \le r+s$, then concatenate these short vectors that are not repeated to produce a keystream

$$p_s q_s \cdots p_u q_u, \text{for } u \le r+s.$$

Note with the knowledge of the keystream, one cannot retrive the irrational number. Thus, the key stream is based on hard mathematical problem of finding a irrational number with sole knowledge of concatenated short vectors obtianed by lattice reduction.

The construction of the cryptosystem is described in the following:

Generating Key exchange using RSA:
Both the sender and reciever need to agree upon a secret key, called key exchange is generated using RSA.

• The sender randomly chooses a large integer $z \in \mathbb{N}$, a non-perfect square number and computes $t \equiv z^e \bmod N$ and sends t to the receiver.
• Now, the reciever using his private key d, computes $z \equiv t^d \bmod N$.

With the knowledge of z, both the parties starts generating the common key as below:

Generating the common key stream using short vectors:
Both sender and receiver agree upon positive integers l, r and s such that $r > s$.
• Sender **A** and receiver **B** computes $\sqrt{z}$ to l decimal places, a very large number.
• Computes short vectors (p_i, q_i) of lattices corresponding to quadratic forms

$$q(x,y) = M\left(\overline{\sqrt{z}}x - y\right)^2 + \frac{1}{M}x^2,$$

for $M = 10^i$, $s \le i \le r$.
• Concatenates the short vectors (p_i, q_i) that are not repeated and obtains a keystream $k = p_s q_s \cdots p_u q_u$, $u \le s + r$. Thus, the key stream

$$k = d_{s1}^p d_{s2}^p \cdots d_{sl_s}^p d_{s1}^q d_{s2}^q \cdots d_{st_s}^q \cdots d_{ut_u}^q,$$

for d_{ij}^p are the digits in p_i and d_{ij}^q are digits in q_i.

Encryption:
• The sender firstly converts his message into numerical equivalents in $\mathbb{Z}_n$ and arrange them in a matrix M of order of his choice(say $p \times q$) $M = [m_{ij}]_{p\times q}$ for m_{ij} is the numerical equivalent of each character.

• The key stream is also arranged as a key matrix $K = [k_{ij}]_{p\times q}$ of order same as that f M, where each entry is $\lceil \log n \rceil$ digits taken at a time from the key stream k.

• Now, enciphering matrix C, is constructed as $C = M + K$, that is, each entry of the matrix is computed as, $[c_{ij}] = [m_{ij}] + [k_{ij}]$ in $\mathbb{Z}_n$ and sends the matrix C to the receiver **B**.

Decryption:
• After receiveing the enciphering matrix, C the key matrix K of order same as that of C, whose each entry is $\lceil \log \mathrm{n} \rceil$ digits taken at a time from the key stream is constructed. Then note $K = [k_{ij}]_{p\times q}$, that is, K is exactly the same as the key matrix constructed by the sender.
• The reciever retrieves the message by computing the message matrix $M = C - K$, that is each entry is computed as, $[m_{ij}] = [c_{ij}] - [k_{ij}]$ in $\mathbb{Z}_n$.

Now, writing the entries of the matrix in a single row and writing its alphabetic equivalents, the receiver reads the message.

Example 1 Suppose sender **A** wants to send the message "ATTACK AT EIGHT IN THE EVENING ON FRIDAY" to receiver **B** in an ecrypted manner and 27-letter alphabet is used with numerical equivalents of $A - Z$ are 0-25 and that of blank space is 26. They both use the public key $(e, N) = (3, 3127)$. Assume that the receiver has his private key $d = 2011$. Both the parties has an understanding on two integers $s = 4$ and $r = 12$.

Generating Key exchange using RSA:
Using public key, sender computes t and sends it to receiver.

$$\begin{aligned} t = z^e \bmod 3127 \\ &= 89^3 \bmod 3127 \\ &= 1394 \end{aligned}$$

Next, using t and his private key d Bob computes z as below:

$$\begin{aligned} z = t^d \bmod 3127 \\ &= 1394^{2011} \bmod 3127 \\ &= 89 \end{aligned}$$

As both the sender and the receiver are ready with the generating key, the start common key generation as below:

Generating the common key stream using short vectors:
Now, both sender and receiver computes and find its decimal expansion corrected to l digits, say 16. Then $\sqrt{89} = 9.4339811320566038$ corrected to 16 decimals. In the next, step both parties find the short vectors of the lattice corresponding to the quadratic form

$$q(x,y) = M\left((\overline{\sqrt{z}})x - y\right)^2 + \frac{1}{M}x^2$$

for $M = 10^4$ to 10^{16}, where $\overline{\sqrt{z}}$ is decimal expansion of $\sqrt{z}$ corrected to the power of M number of decimals. The following table gives the list of short vectors.

Table 1: List of short vectors for $M = 10^4$ to 10^{16}

Sl.No	M	**Unimodular matrix**	Short Vector (p_i, q_i)
1	$M = 10^4$	$U = \begin{bmatrix} 53 & 76 \\ 500 & 717 \end{bmatrix}$	(500,53)
2	$M = 10^5$	$U = \begin{bmatrix} 53 & 818 \\ 500 & 7717 \end{bmatrix}$	(500,53)
3	$M = 10^6$	$U = \begin{bmatrix} 53 & 1030 \\ 500 & 9717 \end{bmatrix}$	(500,53)
4	$M = 10^7$	$U = \begin{bmatrix} 2007 & 977 \\ 18934 & 9257 \end{bmatrix}$	(18934,2007)
5	$M = 10^8$	$U = \begin{bmatrix} 6998 & 9005 \\ 66019 & 84953 \end{bmatrix}$	(66019,6998)
6	$M = 10^9$	$U = \begin{bmatrix} 23001 & 29999 \\ 216991 & 283010 \end{bmatrix}$	(216991,23001)
7	$M = 10^{10}$	$U = \begin{bmatrix} 53000 & 76001 \\ 500001 & 716992 \end{bmatrix}$	(500001,53000)
8	$M = 10^{11}$	$U = \begin{bmatrix} 53000 & 871001 \\ 500001 & 8217007 \end{bmatrix}$	(500001,53000)
9	$M = 10^{12}$	$U = \begin{bmatrix} 977001 & 53000 \\ 9217009 & 500001 \end{bmatrix}$	(9217009,977001)
10	$M = 10^{13}$	$U = \begin{bmatrix} 2007002 & 2984003 \\ 18934019 & 28151028 \end{bmatrix}$	(18934019,2007002)
11	$M = 10^{14}$	$U = \begin{bmatrix} 6998007 & 2007002 \\ 66019066 & 18934019 \end{bmatrix}$	(66019066,6998007)
12	$M = 10^{15}$	$U = \begin{bmatrix} 23001023 & 29999030 \\ 216991217 & 283010283 \end{bmatrix}$	(216991217,23001023)
13	$M = 10^{16}$	$U = \begin{bmatrix} -53000053 & 29999030 \\ -500001500 & 283010283 \end{bmatrix}$	(500001500,53000053)

Now, both parties concatenate the short vectors that are not repeated (p_s, q_s) to (p_{r+s}, q_{r+s}). Then we get,

$k = 500531893420076601969982169912300150$
$000153000921700997700118934019200700$
$266019066699800721699121723001023500$
$12172300102350000150053000053$
.

KEYSTREAM

500531893420076601969982169912300150
000153000921700997700118934019200700
266019066699800721699121723001023500
00150053000053

Encryption:

The sender to communicate the message **"ATTACK AT EIGHT IN THE EVENING ON FRIDAY"**considers the 27 characters for alphabets together with a blank and hence the numerical equivalents of letters of the message are in $\mathbb{Z}_{27}$ and are given as "A-00,T-19,T-19,A-00,C-02,K-10, -26,A-00,T-19, -26,E-04,I-08,G-06,H-07,T-19, -26,I-08,N-13, -26,T-19,H-07,E-04, -26,E-04,V-21,E-04,N-13,I-08,N-13,G-06, -26,O-14,N-13, -26,F-05,R-17,I-08,D-03,A-00,Y-24". The sender represents these numbers in a matrix M of order 5×8, therefore the message matrix M is given as

$$M = \begin{bmatrix} 00 & 19 & 19 & 00 & 02 & 10 & 26 & 00 \\ 19 & 26 & 04 & 08 & 06 & 07 & 19 & 26 \\ 08 & 13 & 26 & 19 & 07 & 04 & 26 & 04 \\ 21 & 04 & 13 & 08 & 13 & 06 & 26 & 14 \\ 13 & 26 & 05 & 17 & 08 & 03 & 00 & 24 \end{bmatrix}$$

Now, he constructs key matrix K by considering $\lceil \log 27 \rceil = 2$ digits taken at a time from k as an enrty of the matrix K of same order as matrix M i.e., 5×8, we have

$$K = \begin{bmatrix} 50 & 05 & 31 & 89 & 34 & 20 & 07 & 66 \\ 01 & 96 & 99 & 82 & 16 & 99 & 12 & 30 \\ 01 & 50 & 00 & 01 & 53 & 00 & 09 & 21 \\ 70 & 09 & 97 & 70 & 01 & 18 & 93 & 40 \\ 19 & 20 & 07 & 00 & 26 & 60 & 19 & 06 \end{bmatrix}$$

Now, the sender computes the cipher matrix C, as

$$(M + K) \bmod 27$$

$$C = (M + K) \bmod 27$$

$$= \begin{bmatrix} 00 & 19 & 19 & 00 & 02 & 10 & 26 & 00 \\ 19 & 26 & 04 & 08 & 06 & 07 & 19 & 26 \\ 08 & 13 & 26 & 19 & 07 & 04 & 26 & 04 \\ 21 & 04 & 13 & 08 & 13 & 06 & 26 & 14 \\ 13 & 26 & 05 & 17 & 08 & 03 & 00 & 24 \end{bmatrix} +$$

$$\begin{bmatrix} 50 & 05 & 31 & 89 & 34 & 20 & 07 & 66 \\ 01 & 96 & 99 & 82 & 16 & 99 & 12 & 30 \\ 01 & 50 & 00 & 01 & 53 & 00 & 09 & 21 \\ 70 & 09 & 97 & 70 & 01 & 18 & 93 & 40 \\ 19 & 20 & 07 & 00 & 26 & 60 & 19 & 06 \end{bmatrix} \bmod 27$$

$$= \begin{bmatrix} 23 & 24 & 23 & 08 & 09 & 03 & 06 & 12 \\ 20 & 14 & 22 & 09 & 22 & 25 & 04 & 02 \\ 09 & 09 & 26 & 20 & 06 & 04 & 08 & 25 \\ 10 & 13 & 02 & 24 & 14 & 24 & 11 & 00 \\ 05 & 19 & 12 & 17 & 07 & 09 & 19 & 03 \end{bmatrix}$$

Now, the sender sends his enciphered message C, to the receiver.

Decryption:

Then, the receiver decrypts C and retrieves M as below:

$$M = (C - K) \bmod 27$$

$$= \begin{bmatrix} 23 & 24 & 23 & 08 & 09 & 03 & 06 & 12 \\ 20 & 14 & 22 & 09 & 22 & 25 & 04 & 02 \\ 09 & 09 & 26 & 20 & 06 & 04 & 08 & 25 \\ 10 & 13 & 02 & 24 & 14 & 24 & 11 & 00 \\ 05 & 19 & 12 & 17 & 07 & 09 & 19 & 03 \end{bmatrix} -$$

$$\begin{bmatrix} 50 & 05 & 31 & 89 & 34 & 20 & 07 & 66 \\ 01 & 96 & 99 & 82 & 16 & 99 & 12 & 30 \\ 01 & 50 & 00 & 01 & 53 & 00 & 09 & 21 \\ 70 & 09 & 97 & 70 & 01 & 18 & 93 & 40 \\ 19 & 20 & 07 & 00 & 26 & 60 & 19 & 06 \end{bmatrix} \bmod 27$$

$$M = \begin{bmatrix} 00 & 19 & 19 & 00 & 02 & 10 & 26 & 00 \\ 19 & 26 & 04 & 08 & 06 & 07 & 19 & 26 \\ 08 & 13 & 26 & 19 & 07 & 05 & 26 & 04 \\ 21 & 04 & 13 & 08 & 13 & 06 & 26 & 14 \\ 13 & 26 & 05 & 17 & 08 & 03 & 00 & 24 \end{bmatrix}$$

Now, writing the entries of the matrix in a single row, we obtain "00-19-19-00-02-10-26-00-19-26-04-08-06-07-19-26-08-13-26-19-07-05-26-04-21-04-13-08-13-08-13-06-26-14-

13-26-050-17-08-03-00-24" whose corresponding alphabets reads as

"**ATTACK AT EIGHT IN THE EVENING ON FRIDAY**".
Thus, the receiver retrieves the message.

We would discuss efficiency and time analysis of our proposed algorithm in the coming section.

IV. EFFICIENCY ANALYSIS

Classical RSA is used for key exchange and if N is the modulus of RSA, then the RSA encryption is about $O(\log_2^2(N))$, and its decryption is $O(\log_2^3(N))$. The time to compute $X = \sqrt{z}$ is about $O(l^3)$, where l is the number of digits in z. The time to compute key stream is obtained by adding time used for the computation of short vectors and concatenation. If we neglect the time for concatenation and consider the time for computing short vectors alone, then the time for key stream is basically the time for LLL algorithm that is $O(w^2 \log w + w^2 \log B)$, where w is the dimension of the lattice and $B = max||b_i||$. Hence the computations are all in polynomial time.

V. CRYPTANALYSIS

The attacker cannot reconstruct initial irrational number even if he obtains many of the digits in key stream also as the short vectors vary according to M, the short vectors do not repeat for long and seperating the digits in the key stream back to short vector is not easy and also as these short vectors are only a subclass of convergents of the irrational, getting back to irrational is not possible with the knowledge of short vectors. One may avoid using the irrationals like π, e with predictable continued fraction expansions.

VI. CONCLUSION

A strong and efficient cryptosystem is build using RSA, a public key cryptosystem for key exchange and a key stream using short vectors of lattices that gives rational approximations of irrational number $\sqrt{z}$ for enciphering and deciphering the huge messages. The efficiency of this system is analysed. In this cryptosystem, each message unit, is enciphered with a different key that helps to withstand attack by frequency analysis. The key stream for enciphering and deciphering is independent of message. The key stream proposed in this paper is efficient than the key stream of [10] based on partial quotients, as the proposed key stream is based on the computation of short vectors that are not recursive unlike partial quotients in the continued fraction expansionon of $\sqrt{z}$, and depends only on choice of M as 10^l for appropriate l.

REFERENCES

[1] Tom M. Apostol, *Introduction to Analytical Number Theory*, Springer-Verlag, New York, 1976.

[2] J. Buchmann, *Introduction to cryptography* , Springer-Verlag , New York, 2004

[3] David M. Burton, *Elementary Number Theory* , Sixth Edition, Tata McGraw-Hill Publishing company limited, New Delhi, India, 2008.

[4] H.Cohen, *A course in Computational Algebraic Number Theory*, Graduate Texts in Math.138. Springer ,1996.

[5] S.C. Coutinho, *The Mathematics of Ciphers*, University Press (India) Private Limited, 2003.

[6] H. Davenport, *The Higher Arithmetic*, Eighth edition, Cambridge University Press, United Kingdom, 2008.

[7] Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Second edition, Springer.

[8] P. Anuradha Kameswari, L. Praveen Kumar, *Encryption on Elliptic Curves over Z_{pq} with Arithmetic on $E(Z_{pq})$ via $E(Z_p)$ and $E(Z_q)$*, IOSR Journal of Mathematics (IOSR-JM), e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 10, Issue 6 Ver. V (Nov - Dec. 2014), 21-29.

[9] P. Anuradha Kameswari, B. Ravitheja, *"Encryption Using Lucas sequences $L(\Delta, pq)$ With Arithmetic on $L(\Delta, pq)$ via $L(\Delta, p)$ and $L(\Delta, q)$* , International Journal of Scientific Research in Mathematical and Statistical Sciences Volume 6, No.1, pp.178-186, 2019

[10] A. M. Kane, *"On the use of Continued Fractions for Stream Ciphers"*, In Proceedings of Security and Management, Las Vegas, USA , 2009.

[11] Neal Koblitz, *A course in Number Theory and cryptography*, Graduate Texts in Mathematics, second edition, Springer.

[12] A.K.Lenstra, H.W. Lenstra and L. Lovasz, *Factoring Polynomials with Rational coefficients*, Math.Ann.261, Springer - Verlag , pp. 515-534, 1982.

[13] Phong Q. Nguyen, Brigitte Valléee (Eds.), *The LLL Algorithm, Survey and Applications*, Springer, 2010.

[14] Nigel P.Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society, Student Texts 41, 1998.

AUTHORS PROFILE

P. Anuradha Kameswari is an Associate Professor, Department of Mathematics, Andhra University. Her research interests are Algebraic Number Theory, Number Theory and Cryptography. She received her Ph.D. in 2000 in Mathematics fromUniversity of Hyderabad.

S B T Sundari Katakam pursued M.Sc. form Andhra University in 2010 and M.Phil. from Andhra University in 2012. She is currently pursing Ph.D. in Andhra University. Her research interests are Number Theory and Cryptography.

