International Journal of Scientific Research in Mathematical and Statistical Sciences
Vol.6, Issue.1, pp.178-186, February (2019)
DOI: https://doi.org/10.26438/ijsrmss/v6i1.178186

Research Paper

E-ISSN: 2348-4519

Encryption Using Lucas sequences $L(\Delta, pq)$ With Arithmetic on $L(\Delta, pq)$ via $L(\Delta, p)$ and $L(\Delta, q)$

P. Anuradha Kameswari[1*], B. Ravitheja[2]

[1]Department of Mathematics, Andhra University,Visakhapatnam - 530003, Andhra Pradesh, India
[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: 09/Feb/2019, Accepted: 22/Feb/2019, Online: 28/Feb/2019

Abstract— In this paper we first established the ring structure on Lucas sequences $L(\Delta, N)$ from the group structure and semigroup structure with the two operations $*$ and $\circ$ respectively. Using the arithmetic of $*$ and $\circ$ on $L(\Delta, N)$ we propose a public key encryption scheme with the pair of Lucas sequences (V_m, U_m) based on the arithmetic of $L(\Delta, pq)$ via $L(\Delta, p)$ and $L(\Delta, q)$. The security of this encryption scheme is based on the discrete log problem of Lucas sequences(V_m, U_m).

Keywords— *Cryptosystem, Lucas sequences, discrete log problem.*

I. INTRODUCTION

Public key cryptosystem based on trapdoor function defined by Lucas sequences $V_n(a, 1)$, was first proposed by Smith and Lennon [8,11] as an analogue to RSA public key cryptosystem. In this paper we construct an encryption scheme using the pair of Lucas sequences (V_n, U_n) in $L(\Delta, N)$ and using the arithmetic of the ring structure on $L(\Delta, N)$ with operations $*$ and $\circ$. This encryption scheme using the pair of Lucas sequences (V_n, U_n) in $L(\Delta, N)$ is based on the arithmetic of $L(\Delta, pq)$ carried via $L(\Delta, p)$ and $L(\Delta, q)$. Basing on this arithmetic we propose a cryptosystem with an advantage of using a same key for multiple communications. The security of the cryptosystem is based on the hardness of discrete log problem of pair of Lucas sequences. The Lucas sequences (V_n, U_n) in this encryption can be computed by using Lucas addition chain for any integer n as in [9]. For any $x, y, x-y$ in the Lucas addition chain we use the formulas $V_{x+y}(a,1) = V_x(a,b)V_y(a,b) - V_{x-y}(a,b)$ and $U_{x+y}(a,1) = U_x(a,b)V_y(a,b) - U_{x-y}(a,b)$

The rest of the paper is organized as follows**:** Section II contains preliminaries on Lucas sequences $L(\Delta, N)$ and their properties. Sections III describes the development of ring structure on $L(\Delta, N)$ and Section IV describes the isomorphism from the ring of $L(\Delta, pq)$ into $L(\Delta, p) \times L(\Delta, q)$ which forms a basis of proposed encryption scheme. Section V contains the construction of proposed encryption based on the arithmetic of $L(\Delta, N)$ carried via $L(\Delta, p)$ and $L(\Delta, q)$. Section VI concludes the construction of encryption with a note on the security of the encryption scheme.

II. PRELIMINARIES

Lucas Sequences and their Properties

Definition 2.1: [2,5,6,8] Let α and b be two integers and α a root of the polynomial $x^2 - ax + b$ in $\mathbf{Q}(\sqrt{\boldsymbol{\Delta}})$ for $\Delta = a^2 - 4b$ a non square, writing $\alpha = \frac{a+\sqrt{\Delta}}{2}$ and its conjugate $\beta = \frac{a-\sqrt{\Delta}}{2}$ we have $\alpha + \beta = a, \alpha\beta = b, \alpha - \beta = \sqrt{\Delta}$ and the Lucas sequences $\{V_k(a,b)\}$ and $\{U_k(a,b)\}, k \geq 0$ are defined as

$$\begin{cases} V_k(a,b) = \alpha^k + \beta^k \\ U_k(a,b) = \frac{\alpha^k - \beta^k}{\alpha - \beta} \end{cases}$$

In Particular, $V_0 = 2,\ V_1 = a,$
and $U_0 = 0 \quad U_1 = 1$

$V_k(a,b)$ and $U_k(a,b)$ are given by following recurrence sequences.

1. $V_k(a,b) = aV_{k-1}(a,b) - bV_{k-2}(a,b)$
2. $U_k(a,b) = aU_{k-1}(a,b) - bU_{k-2}(a,b)$

Lucas sequences satisfying the following properties

1. $V_{2n}(a,b) = (V_n(a,b))^2 - 2b^n$
2. $V_{2n-1}(a,b) = V_n(a,b)V_{n-1}(a,b) - ab^{n-1}$
3. $V_{2n+1}(a,b) = aV_n^2(a,b) - bV_n(a,b)V_{n-1}(a,b) - ab^n$

4. $V_{k+m}(a,b) = \frac{1}{2}(V_k(a,b)V_m(a,b) + \Delta U_k(a,b)U_m(a,b))$
5. $U_{k+m}(a,b) = \frac{1}{2}(U_k(a,b)V_m(a,b) + U_m(a,b)V_k(a,b))$
6. $V_{x+y}(a,b) = V_x(a,b)V_y(a,b) - V_{x-y}(a,b)$
7. $U_{x+y}(a,1) = U_x(a,b)V_y(a,b) - U_{x-y}(a,b)$
8. $U_n^2(a,b) = \frac{V_n^2(a,b)-4}{\Delta}$
9. If $m = p_1^{e_1}, p_2^{e_2} \dots p_r^{e_r}$, such that $(m,\Delta) = 1$ then for $S(m) = lcm[p_i^{e_i-1}\left(p_i - (\frac{\Delta}{p_i})\right)]_{i=1}^{r}$, where $(\frac{\Delta}{p_i})$ is the Legendre's symbol of Δ with respect to the prime p_i,
10. $V_{S(m)}(a,b) \equiv 2b^{\frac{k(1-\varepsilon)}{2}} \text{mod } N$; $U_{S(m)}(a,b) \equiv 0 \text{ mod } N$
11. $V_{S(m)t}(a,b) \equiv 2b^{\frac{k(1-\varepsilon)}{2}} \text{mod } N$; $U_{S(m)t}(a,b) \equiv 0 \text{ mod } N$

In particular for $b = 1$ the above properties can be written as

1. $V_{2n}(a,1) = (V_n(a,1))^2 - 2$
2. $V_{2n-1}(a,1) = V_n(a,1)V_{n-1}(a,1) - a$
3. $V_{2n+1}(a,1) = V_n^2(a,1) - V_n(a,1)V_{n-1}(a,1) - a.$
4. $V_{k+m}(a,1) = \frac{1}{2}(V_k(a,1)V_m(a,1) + \Delta U_k(a,1)U_m(a,1))$
5. $U_{k+m}(a,1) = \frac{1}{2}(U_k(a,1)V_m(a,1) + U_m(a,1)V_k(a,1))$
6. $V_{x+y}(a,1) = V_x(a,1)V_y(a,1) - V_{x-y}(a,1)$
7. $U_{x+y}(a,1) = U_x(a,1)V_y(a,1) - U_{x-y}(a,1)$
8. $U_n^2(a,1) = \frac{V_n^2(a,1)-4}{\Delta}$
9. If $m = p_1^{e_1}, p_2^{e_2} \dots p_r^{e_r}$, such that $(m,\Delta) = 1$ then for $S(m) = lcm[p_i^{e_i-1}\left(p_i - (\frac{\Delta}{p_i})\right)]_{i=1}^{r}$, where $(\frac{\Delta}{p_i})$ is the Legendre's symbol of Δ with respect to the prime p_i,
10. $V_{S(m)}(a,1) \equiv V_0(a,1) \text{mod } N$; $U_{S(m)}(a,1) \equiv U_0(a,1) \text{mod } N$
11. $V_{S(m)t}(a,1) \equiv V_0(a,1) \text{mod } N$; $U_{S(m)t}(a,1) \equiv U_0(a,1) \text{mod } N$

Theorem 2.2 [5]
1. $U_{S(N)t}(a,b) \equiv 0 \text{ mod } N$
2. $V_{S(N)t}(a,b) \equiv 2 \text{ mod } N$ for some integer t

III. Ring structure on Lucas sequences:

In this section we define operations '$*$' and '$\circ$' on $L(\Delta, N)$ and describe the ring structure $(L(\Delta, N), *, \circ)$ of Lucas sequences.

Notation 3.1: Let N be positive integer such that $(N, \Delta) = 1$ and then $\{(V_m, U_m): 1 \leq m \leq S(N)$, where $S(N) = \text{lcm}\{p - (\frac{\Delta}{p}), q - (\frac{\Delta}{q})\}\}$, a set of Lucas sequences is denoted as $L(\Delta, N)$

Definition 3.2: The operation '$*$' on $L(\Delta, N)$ is defined as, for any $(V_k, U_k), (V_m, U_m) \in L(\Delta, N)$, $(V_k, U_k) * (V_m, U_m) = (V_{m+k}, U_{m+k})$.

Definition 3.3: The operation '$\circ$' on $L(\Delta, N)$ is defined as, for any $(V_k, U_k), (V_m, U_m) \in L(\Delta, N)$ $(V_k, U_k) \circ (V_m, U_m) = (V_{mk}, U_{mk})$.

Theorem 3.4: The set $L(\Delta, N)$ forms an abelian group with respect to $*$

Proof. Consider the set $L(\Delta, N) = \{(V_m, U_m): 1 \leq m \leq S(N)$, where $S(N) = \text{lcm}\{p - (\frac{\Delta}{p}), q - (\frac{\Delta}{q})\}\}$ and $*$ be the operation on $L(\Delta, N)$ as above.

$*$ is closed:
By definition, note $L(\Delta, N)$ is closed w.r.t $*$

$*$ is associative:
For any $(V_k, U_k), (V_m, U_m), (V_l, U_l) \in L(\Delta, N)$ we have by the definition

$$\begin{aligned}(V_{k+m}, U_{k+m}) * (V_l, U_l) &= (V_{(k+m)+l}, U_{(k+m)+l}) \\ &= (V_{k+(m+l)}, U_{k+(m+l)}) \\ &= (V_k, U_k) * (V_{m+l}, U_{m+l}) \text{mod } N\end{aligned}$$

Therefore, $L(\Delta, N)$ is associative.

(V_0, U_0) is the identity:
for any $(V_k, U_k) \in L(\Delta, N)$, we have $(V_0, U_0) \in L(\Delta, N)$ such that

$$\begin{aligned}(V_k, U_k) * (V_0, U_0) &= (V_{k+0}, U_{k+0}) \\ &= (V_k, U_k) \\ &= (V_0, U_0) * (V_k, U_k)\end{aligned}$$

Therefore, (V_0, U_0) is the Identity.

Inverse of (V_k, U_k):
For any $(V_k, U_k) \in L(\Delta, N$, we have $(V_{(S(N)-1)k}, U_{(S(N)-1)k}) \in L(\Delta, N)$, and

$$\begin{aligned}(V_k, U_k) * \left(V_{(S(N)-1)k}, U_{(S(N)-1)k}\right) &= \left(V_{k+(S(N)-1)k}, U_{k+(S(N)-1)k}\right) \text{mod } N \\ &= \left(V_{kS(N)}, U_{kS(N)}\right) \text{mod N} \\ &= (2,0)\end{aligned}$$

$= (V_0, U_0) \bmod N$

Therefore,$(V_{(s(N)-1)k}, U_{(s(N)-1)k})$ is the inverse of (V_k, U_k)

$*$ **is commutative:**

$$\begin{aligned}(V_m, U_m) * (V_n, U_n) &= (V_{m+n}, U_{m+n})\\ &= (V_{n+m}, U_{n+m})\\ &= (V_n, U_m) * (V_m, U_n)\end{aligned}$$

Therefore the set $L(\Delta, N) = \{(V_m, U_m): 1 \le m \le S(N),$ where $S(N) = \text{lcm}[(p - \left(\frac{\Delta}{p}\right)), (q - \left(\frac{\Delta}{q}\right))]$ is an abelian group with respect to $*$.

Theorem 3.5 $(\mathrm{V_r}, \mathrm{U_r}) = (\mathrm{V_0}, \mathrm{U_0})$ if and only if $\mathrm{r} \equiv 0 \bmod \mathrm{S(N)}$

Proof. suppose $(V_r, U_r) = (V_0, U_0) \bmod N$

First note by Euler's criterion we have $\Delta^{\frac{p-1}{2}} \equiv \left(\frac{\Delta}{p}\right) \bmod p$, p is smallest such that

$(i)\ \alpha^p \equiv \alpha$ if $(\frac{\Delta}{p}) = 1$

$(ii) \alpha^p \equiv \beta$ if $(\frac{\Delta}{p}) = -1$

as we have for

$$\begin{aligned}\alpha^p &= \left(\frac{\alpha^p + \sqrt{\Delta}^p}{2^p}\right) \bmod p\\ &\equiv \left(\frac{\alpha + \sqrt{\Delta}^p}{2^p}\right) \bmod p\\ &\equiv \left(\frac{\alpha + \Delta^{\frac{p-1}{2}} \Delta^{\frac{1}{2}}}{2}\right) \bmod p\\ &\equiv \left(\frac{\alpha + (\frac{\Delta}{p})\sqrt{\Delta}}{2}\right) \bmod p\\ &\equiv \begin{cases} \frac{\alpha - \sqrt{\Delta}}{2} & \text{if } (\frac{\Delta}{p}) = -1 \\ \frac{\alpha + \sqrt{\Delta}}{2} & \text{if } (\frac{\Delta}{p}) = 1 \end{cases}\\ &\equiv \begin{cases} \beta \text{ if } \left(\frac{\Delta}{p}\right) = -1 \\ \alpha \text{ if } (\frac{\Delta}{p}) = 1 \end{cases}\end{aligned}$$

Now note by (i) and (ii),

$(\mathrm{V_r}, \mathrm{U_r}) = (\mathrm{V_0}, \mathrm{U_0}) \bmod p$

$\Rightarrow \mathrm{V_r} = \mathrm{V_0} \bmod p$ and $\mathrm{U_r} = \mathrm{U_0} \bmod p$

$\Rightarrow \alpha^r + \beta^r \equiv 2 \bmod p$ and $\frac{\alpha^r - \beta^r}{\alpha - \beta} \equiv 0 \bmod p$

$\Rightarrow \alpha^r + \beta^r \equiv 2 \bmod p$ and $\alpha^r \equiv \beta^r \bmod p$

$\Rightarrow 2\alpha^r \equiv 2 \bmod p$

$\Rightarrow \alpha^r \equiv 1 \bmod p$

Now if $(\frac{\Delta}{p}) = 1$ then as (i) implies $(p-1)$ is smallest such that $\alpha^{p-1} \equiv 1 \bmod p$

we have $(p-1)/r$

if $(\frac{\Delta}{p}) = -1$ then as (ii) implies $(p+1)$ is smallest such that $\alpha^{p+1} \equiv \alpha\beta \bmod p$

we have $(p+1)/r$

Therefore for $\alpha^r \equiv 1 \bmod p$ we have $(p-1)/r$ if $(\frac{\Delta}{p}) = 1$ and $(p+1)/r$ if $(\frac{\Delta}{p}) = -1$

$\Rightarrow (p - (\frac{\Delta}{p}))/r.$

For $N = pq$, p and q are primes

$S(N) = \text{lcm}[(p - (\frac{\Delta}{p})), (q - (\frac{\Delta}{q}))]$ we have

$(p - (\frac{\Delta}{p}))/r, (q - (\frac{\Delta}{q}))/r$ ■

$\Rightarrow$ r is a common multiple of$(\mathrm{p} - (\frac{\Delta}{\mathrm{p}})), (\mathrm{p} - (\frac{\Delta}{\mathrm{p}}))$

$\Rightarrow \frac{\text{lcm}\left[\left(\mathrm{p} - \left(\frac{\Delta}{\mathrm{p}}\right)\right), \left(\mathrm{p} - \left(\frac{\Delta}{\mathrm{p}}\right)\right)\right]}{\mathrm{r}}$

$\Rightarrow \mathrm{S(N)/r}$

$\Rightarrow \mathrm{r} \equiv 0 \bmod \mathrm{S(N)}$

conversely suppose $r \equiv 0 \bmod S(N)$

$\Rightarrow r = S(N)t$, for some integer t

$\Rightarrow V_r = V_{S(N)t}$ and $U_r = U_{S(N)t}$

$\Rightarrow V_r \equiv V_0 \bmod N$ and $U_r \equiv U_0 \bmod N$

$\Rightarrow (V_r, U_r) \equiv (V_0, U_0) \bmod N$

$\therefore r \equiv 0 \bmod S(N) \Rightarrow (V_r, U_r) \equiv (V_0, U_0) \bmod N$

Theorem 3.6 $(L(\Delta, N))$ is an abelian group with $O(L(\Delta, N)) = S(N)$.

Proof. By theorem 3.4 we have $L(\Delta, N)$ is abelian group. Now to show $(L(\Delta, N))$ consists of $S(N)$ distinct elements. we have $L(\Delta, N) = \{(V_m, U_m): 1 \le m \le S(N)\}$. If for any s, t such that $1 \le s, t \le S(N)$, $(V_s, U_s) = (V_t, U_t)$ then $V_s = V_t$ and $U_s = U_t$

Now as $V_{s-t} = V_s V_t - \frac{1}{2}(V_s V_t + \Delta U_s U_t)$

we have $V_{s-t} = \frac{1}{2}({V_s}^2 - \Delta {U_s}^2)$

$= \frac{1}{2}({V_s}^2 - \Delta(\frac{V_s^2 - 4}{4}))$

$= 2 \bmod N$

similarly note $U_{s-t} = 0 \bmod N$

$\Rightarrow V_{s-t} = V_0$ and $U_{s-t} = U_0$

Therefore $(V_{s-t}, U_{s-t}) = (V_0, U_0)$ then by theorem 3.5

$\Rightarrow s - t \equiv 0 \bmod S(N)$

$\Rightarrow s \equiv t \bmod S(N)$

$\Rightarrow s = t$ as $0 \le s, t \le S(N)$.

Therefore $L(\Delta, N)$ have $S(N)$ distinct elements.

Theorem 3.7 $\mathrm{L}(\Delta,\mathrm{N})$ with respect to '$\circ$', defined as, for any $(V_k, U_k), (V_m, U_m) \in L(\Delta, N)$ such that $(V_k, U_k) \circ (V_m, U_m)$=$(V_{mk}, U_{mk})$; forms a semogroup with (V_1, U_1) as identity.

Proof. By definition of $\circ$ on $L(\Delta, N)$, note $L(\Delta, N)$ is closed with respect to '$\circ$' and for any (V_k, U_k), (V_m, U_m), $(V_l, U_l) \in L(\Delta, N)$ such that

$$\begin{aligned}
&(V_k, U_k) \circ \big((V_m, U_m) \circ (V_l, U_l)\big) \\
&= (V_k, U_k) \circ (V_{ml}, U_{ml}) \\
&= (V_{k(ml)}, U_{k(ml)}) \\
&= (V_{(km)l}, U_{(km)l}) \\
&= ((V_k, U_k) \circ (V_m, U_m)) \circ (V_l, U_l)
\end{aligned}$$

therefore '$\circ$' is associative, also note '$\circ$' is commutative as

$$\begin{cases} V_{km} = V_{mk} \\ U_{km} = U_{mk} \end{cases}$$

For any $(V_k, U_k) \in L(\Delta, N)$ we have $(V_1, U_1) \in L(\Delta, N)$ such that $(V_k, U_k) \circ (V_1, U_1) = (V_k, U_k)$, (V_1, U_1) is the identity with respect to $\circ$.

Note 1 Any element $(V_k, U_k) \in L(\Delta, N)$ is a unit with respect to '$\circ$' if and only if
$(k, S(N)) = 1$.

Theorem 3.8 The set of all Lucas sequences $(L(\Delta, N), *, \circ)$ forms a ring with respect to $*$ and $\circ$ respectively.

Proof. By Theorem 3.6 $L(\Delta, N)$ forms an abelian group with respect to $*$
and by Theorem 3.7 $L(\Delta, N)$ forms a semigroup with respect to $\circ$
Now note Distributive laws hold on $L(\Delta, N)$,
i.e. The operation $\circ$ distributes with $*$.
For any $(V_k, U_k), (V_m, U_m), (V_l, U_l) \in L(\Delta, N)$

$$\begin{aligned}
&(V_k, U_k) \circ [(V_m, U_m) * (V_l, U_l)] \\
&= (V_k, U_k) \circ [(V_{m+l}, U_{m+l})] \\
&= [V_{k(m+l)}, U_{k(m+l)}] \\
&= [V_{km+kl}, U_{km+kl}] \\
&= [(V_{km}, U_{km}) * (V_{kl}, U_{kl})] \\
&= [((V_k, U_k) \circ (V_m, U_m)) * ((V_k, U_k) \circ (V_l, U_l))]
\end{aligned}$$

$\therefore$ The left distributive holds. Similarly right distributive law that
$[(V_m, U_m) * (V_l, U_l)] \circ (V_k, U_k) = [((V_m, U_m) \circ (V_k, U_k)) * ((V_l, U_l) \circ (V_k, U_k))]$ holds.
Therefore the set of all Lucas sequences $(L(\Delta, N), *, \circ)$ forms ring with respect to $*$ and $\circ$ respectively.

Note 2 For p, q district primes as $(L(\Delta, q), *, \circ)$ and $(L(\Delta, p), *, \circ)$ are two rings, note the cartesian product $(L(\Delta, p) \times L(\Delta, q)$ is also a ring with respect to corresponding $*$ and $\circ$.

IV. ARITHMETIC OF $L(\Delta, N)$ VIA $L(\Delta, p)$ AND $L(\Delta, q)$ FOR $N = pq$

Notation 4.1 For any $(V_m, U_m) \in L(\Delta, N)$, let $V_{m_p} \equiv V_m \bmod p, V_{m_q} \equiv V_m \bmod q$ and $U_{m_p} \equiv U_m \bmod p, U_{m_q} \equiv U_m \bmod q$.

Remark 4.2 For any $(V_m, U_m) \in L(\Delta, N)$, $(V_{m_p}, U_{m_p}), (V_{m_q}, U_{m_q}) \in (L(\Delta, p) \times L(\Delta, q)$ with $m = m_p + S(p)t$ for $0 \leq < \frac{S(q)}{d}$, where $d = \gcd(S(p), S(q))$; which follows from the fact that $L(\Delta, N)$ has $S(N)$ elements which is equal to $\operatorname{lcm}(S(p), S(q))$.

Now we have the following theorem.

Theorem 4.3 The mapping $(V_m, U_m) \to [(V_m^p, U_m^p), (V_m^q, U_m^q)]$ is an isomorphism of $L(\Delta, pq)$ into $L(\Delta, p) \times L(\Delta, q)$.

Proof. For $N = pq, \forall (V_m, U_m) \in L(\Delta, N)$
note $(V_m^p, U_m^p) \in L(\Delta, p)$ and $(V_m^q, U_m^q) \in L(\Delta, q)$
since $(V_m, U_m) \in L(\Delta, N)$, for $r \leq m \leq S(N)$
for $m_p \equiv m \bmod S(p)$, we have $m = m_p + S(p)t, 0 \leq t < \frac{S(q)}{d}$.

$$\begin{aligned}
&\text{therefore } V_m = V_{m_p + S(p)t} \Rightarrow V_m^p \equiv V_m \bmod p \\
&\equiv V_{m_p + S(p)t} \bmod p \\
&\equiv \tfrac{1}{2}\left(V_{m_p} V_{S(p)t} + \Delta U_{m_p} U_{S(p)t}\right) \bmod p \\
&\equiv \frac{1}{2}\left(V_{m_p} V_0 + \Delta U_{m_p} U_0\right) \bmod \mathrm{p} \\
&\equiv V_{m_p + 0} \bmod p \\
&\equiv V_{m_p} \bmod p
\end{aligned}$$

similarly $U_m^p \equiv U_{m_p} \bmod p$ for
$m_p \equiv m \bmod S(p)$
Let $f: L(\Delta, N) \to ((V_{m_p}, U_{m_p}), (V_{m_q}, U_{m_q}))$ be a mapping defined as
$f(V_m, U_m) = (V_{m_p}, U_{m_p}), (V_{m_q}, U_{m_q})$
$Imf = \{((V_{m_p}, U_{m_p}), (V_{m_q}, U_{m_q})) : \forall 1 \leq \mathrm{m} \leq S(pq), m_p = m \bmod S(p), = m \bmod S(q)\}$

f is well defined:
For $(V_m, U_m), (V_k, U_k) \in L(\Delta, N)$ such that

$$\begin{aligned}
&(V_m, U_m) = (V_k, U_k) \\
&\Rightarrow V_m \bmod p = V_k \bmod p, \\
&U_m \bmod p = U_k \bmod p \qquad \blacksquare \\
&\Rightarrow V_m^p = V_k^p, \\
&U_m^p = U_k^p \\
&\Rightarrow (V_m^p, U_m^p) = (V_k^p, U_k^p) \\
&similarly (V_m^q, U_m^q) = (V_k^q, U_k^q) \\
&\Rightarrow [(V_m^p, U_m^p), (V_m^q, U_m^q)] = [(V_k^p, U_k^p), (V_k^q, U_k^q)] \\
&\Rightarrow f(V_m, U_m) = f(V_k, U_k)
\end{aligned}$$

$\therefore$ f is well defined
f is homomorphism:
For $(V_m, U_m), (V_k, U_k) \in L(\Delta, N)$ such that
$f[(V_m, U_m) * (V_k, U_k)]$

$= f[(V_{m+k}, U_{m+k})]$
$= f[(V_m * V_k), (U_m * U_k)]$
$= f[(V_m, U_m) * (V_k, U_k)]$
$= [((V_m^p, U_m^p) * (V_k^p, U_k^p)), ((V_m^q, U_m^q) * (V_k^q, U_k^q))]$
$= [(V_m^p, U_m^p)(V_m^q, U_m^q)] * [(V_k^p, U_k^p), (V_k^q, U_k^q)]$
$= f((V_m, U_m)) * f((V_k, U_k))$

$f[(V_m, U_m) \circ (V_k, U_k)]$
$= f[(V_{mk}, U_{mk})]$
$= f[(V_m \circ V_k), (U_m \circ U_k)]$
$= f[(V_m, U_m) \circ (V_k, U_k)]$
$= [((V_m^p, U_m^p) \circ (V_k^p, U_k^p))((V_m^q, U_m^q) \circ (V_k^q, U_k^q))]$
$= [(V_m^p, U_m^p)(V_m^q, U_m^q)] \circ [(V_k^p, U_k^p), (V_k^q, U_k^q)]$
$= f((V_m, U_m)) \circ f((V_k, U_k))$
$\therefore$ f is homomorphism

f is one-one:
For $(V_m, U_m), (V_k, U_k) \in L(\Delta, N)$ such that
$f(V_m, U_m) = f(V_k, U_k)$
$[(V_m^p, U_m^p), (V_m^q, U_m^q)] = [(V_k^p, U_k^p), (V_k^q, U_k^q)]$

$\therefore$ By Chinese remainder theorem V_m is the unique solution of $V_m \bmod p$, $V_m \bmod p$ and V_k is the unique solution of $V_k \bmod p$, $V_k \bmod p$. Also U_m is the unique solution of $U_m \bmod p$, $U_m \bmod p$ and U_k is the unique solution of $U_k \bmod p$, $U_k \bmod p$
$\therefore V_m = V_k$ and $U_m = U_k$
Hence $(V_m, U_m) = (V_k, U_k)$
$\therefore$ f is one-one

$\therefore L(\Delta, N) \simeq Imf \subseteq L(\Delta, p) \times L(\Delta, q)$

Notation 4.4: Im f or $f(L(\Delta, pq))$ in $L(\Delta, p) \times L(\Delta, q)$ is denoted as $(L(\Delta, p; q))$

The above isomorphism of as $(L(\Delta, N)$ into $L(\Delta, p) \times L(\Delta, q)$ to $(L(\Delta, p; q))$ is depicted in the following table

$L(\Delta,N)$	$L(\Delta,p) \times L(\Delta,q)$						
$L(\Delta,\mathrm{p})$	(V_i,U_i)	(V_0,U_0)	(V_1,U_1)	·	·	·	(V_{m_p},U_{m_p})
$L(\Delta,q)$	(V_0,U_0)	$((V_0,U_0),(V_0,U_0))$	$((V_1,U_1),(V_0,U_0))$	·	·	·	$((V_{m_p},U_{m_p}),(V_0,U_0))$
	(V_1,U_1)	$((V_0,U_0),(V_1,U_1))$	$((V_1,U_1),(V_1,U_1))$	·	·	·	$((V_{m_p},U_{m_p}),(V_1,U_1))$
	·	·	·	·	·	·	·
	·	·	·	·	·	·	·
	·	·	·	·	·	·	·
	$(V_{S(p)},U_{S(p)})$	$((V_0,U_0),(V_{S(p)},U_{S(p)}))$	$((V_1,U_1),(V_{S(p)},U_{S(p)}))$	·	·	·	$((V_{m_p},U_{m_p}),(V_{S(p)},U_{S(p)}))$
	$(V_{S(p)+1},U_{S(p)+1})$	$((V_0,U_0),(V_{S(p)+1},U_{S(p)+1}))$	$((V_1,U_1),(V_{S(p)+1},U_{S(p)+1}))$	·	·	·	$((V_{m_p},U_{m_p}),(V_{S(p)},U_{S(p)}))$
	·	·	·	.	.	.	·
	·	·	·	.	.	.	·
	·	·	·	·	·	·	·
	(V_{m_q},U_{m_q})	$((V_0,U_0),(V_{m_q},U_{m_q}))$	$((V_1,U_1),(V_{m_q},U_{m_q}))$	·	.	·	$((V_{m_p},U_{m_p}),(V_{m_q},U_{m_q}))$

Table 1: $L(\Delta, N) = (L(\Delta, p); L(\Delta, q)) \subseteq L(\Delta, p) \times L(\Delta, q)$

	$L(1{,}5) \times L(4{,}7)$				
$L(1{,}5)$	(V_i, U_i)	(2,0)	(0,1)	(3,0)	(0,4)
$L(4{,}7)$	(2,0)	((2,0),(2,0))	((0,1), (2,0))	((3,0),(2,0))	((0,4), (2,0))
	(1,1)	((2,0), (1,1))	((0,1),(1,1))	((3,0), (1,1))	((0,4),(1,1))
	(6,1)	((2,0),(6,1))	((0,1), (6,1))	((3,0),(6,1))	((0,4), (6,1))
	(5,7)	((2,0), (5,7))	((0,1), (5,7))	((3,0), (5,7))	((0,4), (5,7))
	(6,6)	((2,0), (6,6))	((0,1), (6,6))	((3,5), (6,6))	((0,4), (6,6))
	(1,6)	((2,0), (1,6))	((0,1), (1,6))	((3,0), (1,6))	((0,4), (1,6))

Table 2: Values of $L(\Delta, 35) = (L(\Delta, 5); L(\Delta, 7)) \subseteq L(\Delta, 5) \times L(\Delta, 7)$

In above table, of all values in $L(\Delta, p) \times L(\Delta, q)$, the set of all shaded values is $(L(\Delta, p); L(\Delta, q)) \simeq L(\Delta, N)$

10

$L(\Delta,35)$	$(L(\Delta,5);L(\Delta,7))$
(2,0)	((2,0),(2,0))
(15,1)	((0,1),(1,1))
(13,15)	((3,0),(6,1))
(5,14)	((0,4), (5,7))
(27,20)	((2,0), (6,6))
(15,6)	((0,1),(1,6))
(23,0)	((3,0),(2,0))
(15,29)	((0,4),(1,1))
(27,15)	((2,0),(6,1))
(5,21)	((0,1),(5,7))
(13,20)	((3,0),(6,6))
(15,34)	((0,4),(1,6))

Table 3: $L(\Delta,35)=(L(\Delta,5);L(\Delta,7))\subseteq L(\Delta,5)\times L(\Delta,7)$

Remark 4.5 It follows from the Remark 4.2 that for any (V_{g_p},U_{g_p}) we have $((V_{g_p},U_{g_p}),(V_0,U_0))\in L(\Delta,p)\times L(\Delta,q)$ and this corresponds to $(V_x,U_x)\in L(\Delta,N)$.
i.e. $((V_{g_p},U_{g_p}),(V_0,U_0))=f(V_x,U_x)$ for some $0\le x<S(N)$ if there is an integer $t, 0\le x<\frac{S(q)}{d}$ such that $x=g_p+S(p)t$ and
$x_q\equiv 0 \bmod S(q))$.
symmetrically we have $((V_0,U_0),(V_{g_q},U_{g_q}))$ corresponds to $(V_y,U_y)\in L(\Delta,N)$ for some $0\le y<S(N)$ if there is an integer $t, 0\le y<\frac{S(p)}{d}$ such that $y=g_q+S(p)t$ and $x_p\equiv 0 \bmod S(p)$.

We have $L(\Delta,N)\cong L(\Delta,p;q)$, using this isomorphism an Encryption scheme is given in the next section.
In the following, we give an algorithm for computations of Lucas sequences (V_n,U_n) involving operations '$*$' as $(V_k,U_k)*(V_m,U_m)=(V_{k+m},U_{K+m})$ and '$\circ$' as $(V_k,U_k)\circ(V_m,U_m)=(V_{km},U_{Km})$

Algorithm:
step 0: (Initialize) Set $N\leftarrow\frac{n}{2^{k-i}}$ where $k=\lfloor\log n\rfloor, i=0,1,2,\dots,k$
$X\leftarrow 0, Y\leftarrow 1, Z\leftarrow Y+1$
step 1: (Value N) $N\leftarrow\frac{n}{2^{k-i}}$ and determine whether N is even or odd, if N is even skip to
step 4.
step 2: set $X\leftarrow 2Y, Y\leftarrow X+1$ and $Z\leftarrow 2z$
step 3: $[N=n]$, if $N=n$ the algorithm terminates with Y as the answer.
step 4: set$X\leftarrow X+Y, Y\leftarrow 2Y$, $Z\leftarrow Y+1$ and return to step 1.
step 5: [initialize] set $V_0(a,1)=2, V_1(a,1)=a, U_0(a,1)=0, U_1(a,1)=1$
step 6: For i from 0 to k
set $V_n\leftarrow V_X, V_Y$ and V_Z
set $V_n\leftarrow U_X, U_Y$ and U_Z
set $n\leftarrow i+j$ and compute $V_{i+j}(a,1)\leftarrow V_i(a,1)V_j(a,1)-V_{i-j}(a,1)$
set $n\leftarrow i+j$ and compute $U_{i+j}(a,1)\leftarrow U_i(a,1)V_j(a,1)-U_{i-j}(a,1)$
step 7: For given values k,m
compute $(V_k,U_k)*(V_m,U_m)=(V_{k+m},U_{K+m})$
compute $(V_k,U_k)\circ(V_m,U_m)=(V_{km},U_{Km})$
step 8: For given values k,m,l compute
$(V_k,U_k)\circ((V_m,U_m)*(V_l,U_l))=(V_{k(m+l)},U_{k(m+l)})$
compute
$(V_k,U_k)*((V_m,U_m)*(V_l,U_l))=(V_{k+m+l},U_{K+m+l})$
Therefore this algorithm is used to evaluating the Lucas sequences (V_n,U_n) and computations involving the proposed cryptosystem which is described in the following.

V. ENCRYPTION USING LUCAS SEQUENCES $L(\Delta,pq)$ WITH ARITHMETIC OF $*$ and $\circ$ ON $L(\Delta,pq)$ VIA $L(\Delta,p)$ AND $L(\Delta,q)$:

In the following Cryptosystem sender and receiver generate a common key basing on discrete log problem of Lucas sequences modulo N and then start the communication.
Generating common key:
1. Receiver chooses primes p,q and select the Lucas polynomial $x^2-ax+1\in L(\Delta,N)$.
Choose a random integer t such that $T=(V_t,U_t)$ in $L(\Delta,N)$ and $T_p=\left(V_t^p,U_t^p\right)\in L(\Delta,p), T_q=(V_t^q,U_t^q)\in L(\Delta,q)$ and makes (N,T) public.
2. Sender chooses a random integer r such that $R=(V_r,U_r)$ and makes $(N,R\circ T)=(N,(V_r,U_r)\circ(V_t,U_t))$ public.
3. Sender and receiver agree upon secret key $R\circ T$
4. Public Key: a, $L(\Delta,N)$, (N,T), $(N,R\circ T)$ and a_i,b_i
Before start the communication receiver do the following.
Receiver chooses a random number $g, 0\le g\le S(N)$ and (V_g,U_g) then and fixes $G^p=((V_g^p,U_g^p),(V_0^q,U_0^q))\in$

$L(\Delta, N), G^q = ((V_0^p, U_0^p), (V_g^q, U_g^q)) \in L(\Delta, N)$.
Also computes $C = [R \circ (G^q * T^{-1})]$ and $D = [R \circ (G^p * T^{-1})]$

$$C = [R \circ (G^q * T^{-1})]$$
$$= [((V_r^p, U_r^p), (V_r^q, U_r^q)) \circ ((V_0^p, U_0^p), (V_g^q, U_g^q)) * ((V_{-t}^p, U_{-t}^p), (V_{-t}^q, U_{-t}^q))]$$
$$= [((V_r^p, U_r^p), (V_r^q, U_r^q)) \circ ((V_0^p, U_0^p) * (V_{-t}^p, U_{-t}^p)), ((V_g^q, U_g^q) * (V_{-t}^q, U_{-t}^q))]$$

$$= [((V_r^p, U_r^p), (V_r^q, U_r^q)) \circ ((V_{-t}^p, U_{-t}^p), (V_{g-t}^q, U_{g-t}^q))]$$
$$= [((V_r^p, U_r^p) \circ (V_{-t}^p, U_{-t}^p)), ((V_r^q, U_r^q) \circ (V_{g-t}^q, U_{g-t}^q))]$$
$$= [((V_{-rt}^p, U_{-rt}^p), (V_{r(g-t)}^q, U_{r(g-t)}^q))]$$

By using the Chinese remainder theorem computes (V_c, U_c) by solving $V_c^p = V_{-rt} \bmod p, V_c^q = V_{r(g-t)} \bmod q$; $U_c^p = U_{-rt} \bmod p, U_c^q = U_{r(g-t)} \bmod q$ and makes the pair $C = ((V_c, U_c))$ public

and

$$D = [Ro(G^p * T^{-1})]$$
$$= [((V_r^p, U_r^p), (V_r^q, U_r^q)) \circ ((V_g^p, U_g^p), (V_0^q, U_0^q)) * ((V_{-t}^p, U_{-t}^p), (V_{-t}^q, U_{-t}^q))]$$
$$= [((V_r^p, U_r^p), (V_r^q, U_r^q)) \circ ((V_g^p, U_g^p) * (V_{-t}^p, U_{-t}^p)), ((V_0^q, U_0^q) * (V_{-t}^q, U_{-t}^q))]$$
$$= [((V_r^p, U_r^p), (V_r^q, U_r^q)) \circ ((V_{g-t}^p, U_{g-t}^p), (V_{-t}^q, U_{-t}^q))]$$
$$= [((V_r^p, U_r^p) \circ (V_{g-t}^p, U_{g-t}^p)), ((V_r^q, U_r^q) \circ (V_{-t}^q, U_{-t}^q))]$$
$$= [((V_{r(g-t)}^p, U_{r(g-t)}^p), (V_{-rt}^q, U_{-rt}^q))]$$

By using the Chinese remainder theorem computes (V_d, U_d) by solving $V_d^p = V_{r(g-t)} \bmod p, V_d^q = V_{-rt} \bmod q$; $U_d^p = U_{r(g-t)} \bmod p, U_d^q = U_{-rt} \bmod q$ and makes the pair $D = ((V_d, U_d))$ public

Encryption:

Let (V_m, U_m) be the Lucas equivalent to the message M. Sender chooses random pair of Lucas sequences $(V_m, U_m) \bmod N$ and represents the message as $M = (V_m, U_m)$.
Also sender encrypts the message M by computing $\tilde{C} = C * (V_{rt}, U_{rt}) * (V_m, U_m)$ and $\widetilde{D} = D * (V_{rt}, U_{rt}) * (V_m, U_m)$ as follows

$$\widetilde{C} = [C * ((V_{rt}, U_{rt}) * (V_m, U_m))]$$
$$= [(V_c, U_c) * ((V_{rt}, U_{rt}) * (V_m, U_m))]$$
$$= [(V_c, U_c) * (V_{rt+m}, U_{rt+m})]$$
$$= [(V_{c+rt+m}, U_{c+rt+m})]$$

and

$$\widetilde{D} = [D * ((V_{rt}, U_{rt}) * (V_m, U_m))]$$
$$= [(V_d, U_d) * ((V_{rt}, U_{rt}) * (V_m, U_m))]$$
$$= [(V_d, U_d) * (V_{rt+m}, U_{rt+m})]$$
$$= [(V_{d+rt+m}, U_{d+rt+m})]$$

Sender makes $(\tilde{C}, \widetilde{D})$ public.

Decryption:

Receiver decrypts the message M by computing $M_c = \tilde{C} * ((V_{-rt}, U_{-rt}) * (V_{-c}, U_{-c}))$ and $M_d = \widetilde{D} * ((V_{rt}, U_{rt}) * (V_{-d}, U_{-d}))$ as follows

$$M_c = \tilde{C} *_c ((V_{-rt}, U_{-rt}) *_c (V_{-c}, U_{-c}))$$

$$= [(V_{\tilde{c}}^p, U_{\tilde{c}}^p), (V_{\tilde{c}}^q, U_{\tilde{c}}^q)] *_c [((V_{-rt}^p, U_{-rt}^p), (V_{-rt}^q, U_{-rt}^q)) *_c ((V_{-c}^p, U_{-c}^p), (V_{-c}^q, U_{-c}^q))]$$

$$= [(V_{\tilde{c}}^p, U_{\tilde{c}}^p), (V_{\tilde{c}}^q, U_{\tilde{c}}^q)] *_c [((V_{-rt}^p, U_{-rt}^p) * (V_{-c}^p, U_{-c}^p)), ((V_{-rt}^q, U_{-rt}^q) * (V_{-c}^q, U_{-c}^q))$$

$$= [(V_{\tilde{c}}^p, U_{\tilde{c}}^p), (V_{\tilde{c}}^q, U_{\tilde{c}}^q)] *_c [(V_{-(rt+c)}^p, U_{-(rt+c)}^p), (V_{-(rt+c)}^q, U_{-(rt+c)}^q)]$$
$$= [(V_{\tilde{c}}^p, U_{\tilde{c}}^p) * (V_{-(rt+c)}^p, U_{-(rt+c)}^p), (V_{\tilde{c}}^q, U_{\tilde{c}}^q) * (V_{-(rt+c)}^q, U_{-(rt+c)}^q)]$$
$$= [(V_{\tilde{c}-rt-c}^p, U_{\tilde{c}-rt-c}^p) * (V_{\tilde{c}-rt-c}^q, U_{\tilde{c}-rt-c}^q)]$$

and

$$M_d = \widetilde{D} *_c ((V_{-rt}, U_{-rt}) *_c (V_{-d}, U_{-d}))$$

$$= [(V_{\tilde{d}}^p, U_{\tilde{d}}^p), (V_{\tilde{d}}^q, U_{\tilde{d}}^q)] *_c [((V_{-rt}^p, U_{-rt}^p), (V_{-rt}^q, U_{-rt}^q)) *_c ((V_{-d}^p, U_{-d}^p), (V_{-d}^q, U_{-d}^q))]$$

$$= [(V_{\tilde{d}}^p, U_{\tilde{d}}^p), (V_{\tilde{d}}^q, U_{\tilde{d}}^q)] *_c [((V_{-rt}^p, U_{-rt}^p) * (V_{-d}^p, U_{-d}^p)), ((V_{-rt}^q, U_{-rt}^q) * (V_{-d}^q, U_{-d}^q))$$
$$= [(V_{\tilde{d}}^p, U_{\tilde{d}}^p), (V_{\tilde{d}}^q, U_{\tilde{d}}^q)] *_c [(V_{-(rt+d)}^p, U_{-(rt+d)}^p), (V_{-(rt+d)}^q, U_{-(rt+d)}^q)]$$
$$= [(V_{\tilde{d}}^p, U_{\tilde{d}}^p) * (V_{-(rt+d)}^p, U_{-(rt+d)}^p), (V_{\tilde{d}}^q, U_{\tilde{d}}^q) * (V_{-(rt+d)}^q, U_{-(rt+d)}^q)]$$
$$= [(V_{\tilde{d}-rt-d}^p, U_{\tilde{d}-rt-d}^p) * (V_{\tilde{d}-rt-d}^q, U_{\tilde{d}-rt-d}^q)]$$

Here $M_c \bmod p = (V_{\tilde{c}-rt-c}^p, U_{\tilde{c}-rt-c}^p)$, $M_d \bmod q = (V_{\tilde{d}-rt-d}^q, U_{\tilde{d}-rt-d}^q)$ and retrieve the message M using the Chinese remainder theorem by solving $V_{\tilde{c}-rt-c} \bmod p, V_{\tilde{d}-rt-d} \bmod q$; $U_{\tilde{c}-rt-c} \bmod p, U_{\tilde{d}-rt-d} \bmod q$.
The message $M = (V_m, U_m) \bmod N$ can be represented as $M = \sum_{i=1}^{r} a_i V_m(a, 1) + b_i U_m(a, 1)$.

Example Sender and receiver generate a common key basing on discrete log problem of Lucas sequences $x^2 - 15x + 1 \in L(11,35)$ for $a = 15$ and the order of $L(\Delta, N)$ is $S(N) = 12$.

Generating common key:

1. Receiver chooses random primes $p = 5$ and $q = 7$ and select the Lucas polynomial $x^2 - 15x + 1 \in L(11,35)$. Choose $T = (27,20)$ for some integer 4 in $L(11,35)$ and $T^5 = (2,0) \in L(1,5), T^7 = (6,6) \in L(4,7)$ and makes $(35, (27,20))$ public.

2. Sender chooses $R = (5,14)$, for $r = 3$ and makes $(35, (5,14) \circ (27,20) = (35, (2,0))$ public.
3. Sender and receiver agree upon secret key $R \circ T = ((5,14) \circ (27,20)) = (2,0)$.
4. Public Key: $L(11,35)$, $(35, (27,20))$, $(35, (2,0))$ and $a_1 = 2, b_1 = 3$.

Before start the communication receiver do the following.
Receiver chooses random number $g = 7$ and fixes $G^5 = ((V_6^5, U_6^5), (V_0^7, U_0^7)) = ((3,0), (2,0))$ and $G^7 = ((V_0^5, U_0^5), (V_6^7, U_6^7)) = ((2,0), (2,0))$.

Also computes $C = [R \circ (G^7 * T^{-1})]$ and $D = [R \circ (G^5 * T^{-1})]$

$C = [Ro(G^7 * T^{-1})]$
$= [(0,4), (5,7) \circ ((2,0), (2,0) * (2,0), (6,1))]$
$= [(0,4), (5,7) \circ ((2,0) * (2,0), (2,0) * (6,1))]$
$= [(0,4), (5,7) \circ (2,0), (6,1)]$
$= [(0,4) \circ (2,0), (5,7) \circ (5,7)]$
$= [(2,0), (2,0)]$

By using the Chinese remainder theorem, solving the following congruences:

$x \equiv 2 \bmod 5$
$x \equiv 2 \bmod 7$
and
$y \equiv 0 \bmod 5$
$y \equiv 0 \bmod 7$

then $C = (2,0)$

$D = [Ro(G^5 * T^{-1})]$
$= [(0,4), (5,7) \circ ((3,0), (2,0) * (2,0), (6,1))]$
$= [(0,4), (5,7) \circ ((3,0) * (2,0), (2,0) * (6,1))]$
$= [(0,4), (5,7) \circ (3,0), (6,1)]$
$= [(0,4) \circ (3,0), (5,7) \circ (6,1)]$
$= [(3,0), (2,0)]$

By using the Chinese remainder theorem, solving the following congruences:

$x \equiv 3 \bmod 5$
$x \equiv 2 \bmod 7$

and

$y \equiv 0 \bmod 5$
$y \equiv 0 \bmod 7$

$\therefore D = (23,0)$

then C, D are public.

Encryption:
Sender sequences represents the message as (V_{19}, U_{19}) for $m = 19$ and $(V_{19}, U_{19}) = (15,29)$.
Also Sender encrypts the message M by computing $\tilde{C} = C * (V_{12}, U_{12}) * (V_{19}, U_{19}))$ and $\widetilde{D} = D * ((V_{12}, U_{12}) * (V_{19}, U_{19}))$ as follows.

$\tilde{C} = [(V_0, U_0) * (V_{12}, U_{12}) * (V_{19}, U_{19}))]$
$= [(2,0) * ((20,34) * (2,0))]$
$= [(2,0) * (15,29)]$
$= (15,29)$
and
$\widetilde{D} = [(V_6, U_6) * ((V_{12}, U_{12}) * (V_{19}, U_{19}))] = [(23,0) * ((20,34) * (2,0))]$
$= [(23,0) * (15,29)]$
$= (1,1)$

Sender makes $(\tilde{C}, \widetilde{D})$ public.

Decryption:
Receiver decrypts the message M by computing $M_c = \tilde{C} * ((V_{-rt}, U_{-rt}) * (V_{-c}, U_{-c}))$ and $M_d = \widetilde{D} * ((V_{rt}, U_{rt}) * (V_{-d}, U_{-d}))$ as follows

$M_c = [((0,4), (1,1))] *_c [((2,0), (2,0)) *_c ((2,0)(2,0))]$
$= [((0,4), (1,1))] *_c [((2,0) * (2,0)), ((2,0) * (2,0))]$
$= [((0,4) * (2,0)), ((1,1) * (2,0))]$
$= [((0,4), (1,1))]$
and
$M_d = [((0,1), (1,1))] *_c [((2,0), (2,0)) *_c ((3,0)(2,0))]$
$= [((0,1), (1,1))] *_c [((2,0) * (3,0)), ((2,0) * (2,0))]$
$= [((0,1) * (3,0)), ((1,1) * (2,0))]$
$= [((0,4), (1,1))]$

Here $M_c \bmod 5 = (0,4)$, $M_d \bmod 7 = (1,1)$ and retrieve the message $M = 117$ as $M = a_1 V_{m_1} + b_1 U_{m_1} = 2.15 + 3.29 = 117$ by using the Chinese remainder theorem for solving

$x \equiv 0 \bmod 5$
$x \equiv 1 \bmod 7$

and

$y \equiv 4 \bmod 5$
$y \equiv 1 \bmod 7$

VI. CONCLUSION

The encryption scheme with Lucas sequences proposed in this paper is based on arithmetic of $*, \circ$ on $L(\Delta, pq)$ carried via arithmetic of $*, \circ$ on $L(\Delta, p)$ and $L(\Delta, q)$. This was adapted by exploiting the isomorphism from the ring $L(\Delta, N)$ to ring $L(\Delta, p, q)$ where $L(\Delta, p, q)$ is a subset of $L(\Delta, p) \times L(\Delta, q)$. In this encryption scheme, the sender and the receiver generate a common key basing on discrete log problem of (V_m, U_m) in $L(\Delta, N)$. The sender also uses a private key each time a message M is sent to receiver. The security of this encryption is based on factorization of N and also on the discrete log of Lucas sequences (V_m, U_m) with a possibility of choosing large m, which there by increases the security.

REFERENCES

[1] Zulkarnian Md Ali, M.Othman, M.R.M. Said, M.N.Sulaiman, *Computation of cryptosystem based on Lucas functions using addition chain*, IEEE, (2010),1082-1086.

[2] L.E.Dickson, *History of the Theory of Numbers*, volume 1, Chelsea publishing company, New York, 1919.

[3] Daniel Bleinchenbacher, *Efficiency and security of cryptosystems based on Number Theory*, Ph.D thesis,(1964)

[4] D.E.Knuth, LU- *The art of computer programming*, Volume II: Seminumerical Algorithms, Third Edition,Addison-Wesley(1998)

[5] D.H.Lehmer, *An Extendeds theory of Lucas functions*, Annals of Math.,31(1930)pp419-448.

[6] Peter L. Montgomery, *evaluating recurrences of the form* $X_{m+n} = f(X_m, X_n, X_{m-n})$ *via Lucas chains*, January,(1992)

[7] 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), Volume 10, Issue 6 Ver. V (Nov - Dec. 2014), PP 21-29.

[8] P.J.Smith, G.J.J.Lennon, *LUC:a new public key cryptosystem*, Ninth IFIP Sympoiusm on Computer Science Security, Elsevier Science Publications(1993)103-117.

[9] P. Anuradha Kameswari, B. Ravitheja, *Addition Chain for Lucas Sequences with Fast Computation Method*, International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9413–9419.

[10] P. Anuradha Kameswari, T. Surendra and B.Ravitheja, *Shank's Baby-step Gaint-step Attack extended to discrete log with Lucas sequences*, IOSR Journal of Mathematics,Vol 12, Issue 1, pp 09-16, 2016.

[11] Ravitheja.B, *RSA-like cryptosystem based on Lucas sequences*, Dissertation, Andhra University,(2015)

[12] Rishav Upadhyay, Shibaji Kundu, *A Preliminary Approach to Daily Use Cryptography*, International Journal of Computer Science and Engineering, Vol. 3, Issue 6, pp 14-16.

AUTHORS PROFILE

Dr. P. Anuradha Kameswari is an Associate Professor in 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 from University of Hyderabad

Mr. Ravitheja Badugu pursued M.Sc. form Nagarjuna University in 2012 and M.Phil. from Andhra University in 2015. He is currently pursing Ph.D. in Andhra University. His research interests are Number Theory and Cryptography. Mr. Ravitheja Badugu thanks the University Grants Commission, India for research support under the scheme of Rajiv Gandhi National Fellowship.