Malaysian Journal of Mathematical Sciences **1(1)**: 63 - 81 (2007)

# The Quartic Analog to the RSA Cryptosystem

**Wong Tze Jin, Mohamad Rushdan Md. Said,**
**Kamel Ariffin Mohd. Atan & Bekbaev Ural**
*Institute for Mathematical Research, Universiti Putra Malaysia,*
*43400 UPM, Serdang, Selangor, Malaysia*
*E-mail : tjwong1979@gmail.com, mrushdan@fsas.upm.edu.my*

## ABSTRACT

This paper reports an investigation into a public key cryptosystem, which is derived from a fourth order linear recurrence relation and is based on the Lucas function. This cryptosystem is also analogous to the RSA, LUC and $LUC_3$ cryptosystems. The explicit formulation involves a generalisation of the Euler Totient function, which underlie the algebra of the RSA cryptosystem.

**Keywords**: Quartic Polynomial, Resolvent Cubic Polynomial,Fourth Order Lucas Sequence, Sixth Order Lucas Sequence, Euler Totient Function, Quartic Cryptosystem

## INTRODUCTION

The most striking development in the history of cryptography was when Diffie and Hellman (1976) published *New Directions in Cryptography.* Rivest *et al.* (1978) discovered the first practical public-key encryption and signature scheme, now referred to as RSA. The RSA scheme is based on another difficult mathematical problem, which is the intractability of factoring large integers. This application of a difficult mathematical problem to cryptography revitalized efforts to find more efficient methods for factoring. Therefore, the study aimed to develop a new cryptosystem analog to the RSA, LUC and $LUC_3$ cryptosystems. Apart from the advancement in knowledge, a prime motivation to develop a new cryptosystem is the possibility that $LUC_4$ cryptosystem is more secure than RSA, LUC and $LUC_3$ cryptosystems. This is because the calculations of $LUC_4$ cryptosystem are more complicated than those of RSA, LUC and $LUC_3$ cryptosystems.

*The RSA Cryptosystem*

In the RSA cryptosystem (Rivest *et al.*, 1978), an encryption key ($e$, $N$)is being used, where $e$ and $N$ are positive integers and $N$ is the product of two large primes $p$ and $q$, which are not revealed. The decryption key is the pair of positive integers ($d$, $N$), where $d$ is determined by . Here, the Euler totient function is computered as $\phi(N) = (p-1)(q-1)$. For maximum security, $p$ and $q$ are of equal length.

To encrypt the message, the sender raises the message $M$ to the $e$-th power modulo $N$. To decrypt the ciphertext, it is raised to another power $d$, again modulo $N$. The encryption and decryption algorithms $E$ and $D$ are thus:

$C \equiv E(M) \equiv M^e \bmod N$, for a message $M$.
$M \equiv D(C) \equiv C^d \bmod N$, for a ciphertext $C$.

Note that encryption does not increase the size of a message. Both the message and the ciphertext are integers in the range 0 to $N$-1. Each user makes the encryption key public, and keeps the corresponding decryption key private. Then the encryption key, $e$, is randomly choosen such that $e$ and $(p-1)(q-1)$ are relatively prime.

*LUC Cryptosystem*

Suppose $N$ and $e$ are two chosen numbers, with $N$ the product of two different odd primes, $p$ and $q$. The number $e$ must be chosen so it is relatively prime to $(p-1)(q-1)(p+1)(q+1)$. Let $M$ be a message, which is less than $N$, and relatively prime to $N$. This is not a real restriction on $M$, because $p$ and $q$ are large enough such that the probability of the secret key being divisible by one of them is less than the probability of the secret key being revealed by some unforeseen event. Then, the encryption of LUC cryptosystem (Smith and Lennon, 1993) can be defined as:

$$f_{LUC}(M) = V_e(M,1) \bmod N$$

where $V_e$ is a Lucas function. This is the LUC public key process, giving an encrypted message, $M'$. To define the matching decryption key process, a number $d$ is reduced such that $de \equiv 1 \bmod S(N)$, where $S(N) = \text{lcm}\left((p - \left(\frac{D}{p}\right), (q - \left(\frac{D}{q}\right)\right))$, $D=(M')-4$ and $\left(\frac{D}{p}\right)$, $\left(\frac{D}{q}\right)$ are the Legendre symbols of $D$ with respect to $p$ and $q$ and lcm is the least common multiple.

The decryption is then the same as the encryption keys processes, with $e$ replaced by $d$. The fact that $M < N$,

$$M \equiv V_d(V_e(M,1) \bmod N, 1) \bmod N,$$

and the decryption key process and encryption key process are inversions of each other by the symmetry between $e$ and $d$.

*$LUC_3$ Cryptosystem*

As in the RSA and LUC cryptosystems, the strength of the cubic analogue to the RSA cryptosystem (Said & Loxton, 2003) depends on the difficulty of factoring large numbers. Thus, it is necessary to pick two large secret primes $p$ and $q$, the product $N$ of which is part of the encryption key. The encryption key is $(e, N)$ which is made public. Note that, $e$ must be chosen so that it is relatively prime to the function $\Phi(N) = \overline{pq}$ because it is necessary to solve the congruence $ed \equiv 1 \bmod F(N)$ to find the decryption key $d$. The Euler Totient function is:

$$\Phi(N) = p_1^{b_1-1}\,\overline{p_1}\,p_2^{b_2-1}\,\overline{p_2}\cdots p_r^{b_r-1}\,\overline{p_r}$$

where

$$\overline{p_i} = \begin{cases} p_i^{\,2} + p_i + 1 & \text{if } f(x) \text{ is of type } t[3] \bmod p_i \\ p_i^{\,2} - 1 & \text{if } f(x) \text{ is of type } t[2,1] \bmod p_i \\ p_i - 1 & \text{if } f(x) \text{ is of type } t[1] \bmod p_i \end{cases}$$

and *f(x)* is a cubic polynomial $f(x) = x^3 - Px^2 + Qx - R$. In practice, since F (N) depends on this type of an auxiliary polynomial, we choose *e* prime to *p*-1, *q*-1, *p*+1, *q*+1, $p^2+p+1$, and $q^2+q+1$ to cover all possible cases.

With these preliminary observations, a public-key cryptosystem is set up based on the cubic recurrence sequence $V_n$ derived from the cubic polynomial $x^3-Px^2+Qx-R=0$. The encryption function is defined by $E(P,Q) = (V_e(P,Q,1),Ve(Q,P,1)) \equiv (C_1,C_2) \bmod N$, where $N = pq$ as above, $V_e(P,Q,l)$ is the *e*-th term of the cubic recurrence defined by $V_{n+3} = PV_{n+2}\ QV_{n+1} + V_n \bmod N$ with initial values $V_0 = 3$, $V_1 = P$ and $V_2 = P^2 - 2Q$, and *(P, Q)* constitutes the message. At the same time, *P* and *Q* are coefficients for cubic polynomial $f(x) = x^3 - Px^2 + Qx - 1$. The encryption key is (*e*, *N*).

The decryption key is (*d*, *N*) where *d* is the inverse of *e* modulo F (*N*). To decrypt the message, the receiver must know or be able to compute F(*N*) and then calculate

$$D(C_1,C_2) = (V_d(C_1,C_2,1),\ V_d(C_2,C_1,1)) \equiv (P,Q) \bmod N$$

which recovers the original message (*P, Q*).

## HIGH ORDER LINEAR RECURRENCE SEQUENCE OF LUCAS FUNCTION

A second order linear recurrence of Lucas function is a sequence of integers $T_n$ defined by $T_0 = a$, $T_1 = b$ (*a* and *b* integers) and $T_n = PT_{n-1} - QT_{n-2}$, where *P* and *Q* are coefficients in Quadratic polynomial, $x^2-Px+Q=0$. The extensions of this result are fourth and sixth order linear recurrence sequence.

*Fourth Order Lucas Sequence*

By analogy with the Lucas sequence, we consider the quartic polynomial

$$x^4 - Px^3 + Qx^2 - Rx + S = 0$$

with integer coefficients *P, Q, R,* and *S* and roots $\beta_1,\beta_2,\beta_3,\beta_4$; where $P = \sum_{i=1}^{4} \beta_i$ ,

$Q = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \beta_i\beta_j$ , $R = \sum_{i=1}^{2} \sum_{j=2;\, i<j<k}^{3} \sum_{k=3;\, i,\, j<k}^{4} \beta_i\beta_j\beta_k$ and $S = \prod_{i=1}^{4} \beta_i$ .

The factorization of $f(x)=x^4-Px^3 + Qx^2 - Rx + S$ modulo $p$ is unique and can be classified into five major types as follows:

i. type $t[4]$ -- $f(x)$ is irreducible,
ii. type $t[3,1]$ -- $f(x)$ factors as an irreducible cubic times a linear factor,
iii. type $t[2,1]$ -- $f(x)$ factors as an irreducible quadratic times two linear factors,
iv. type $t[2]$ -- $f(x)$ factors as two irreducible quadratic,
v. type $t[1]$ -- $f(x)$ factors into four linear factors.

Corresponding to the Quartic polynomial, we define the fourth order linear recurrence relation as below.

Proposition 1: Let $V_n(P,Q,R,S) = \sum_{i=1}^{4} \beta_i^n$ ,with initial values $V_0(P,Q,R,S) = 4$, $V_1(P,Q,R,S) = P$, $V_2(P,Q,R,S) = P^2-2Q$, and V3(P,Q,R,S) = $P^3$-3PQ + 3R.
Then, the fourth order Lucas sequence is

$V_n(P, Q, R, S) = PV_{n-1} - QV_{n-2} + RV_{n-3} - SV_{n-4}$, for $n > 4$

**Proof**

The Principle of Mathematical Induction is used to prove the above proposition. First, it must be established that $V_4$ is true.

$$V_4 = \sum_{i=1}^{4}\beta_i^4 = \sum_{i=1}^{4}\beta_i \sum_{i=1}^{4}\beta_i^3 - \sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\beta_i\beta_j\sum_{i=1}^{4}\beta_i^2 + \sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\beta_i\beta_j\beta_k\sum_{i=1}^{4}\beta_i - 4\prod_{i=1}^{4}\beta_i$$
$$= PV_3 - QV_2 + RV_1 - SV_0$$

Then, supposing

$$V_n(P,Q,R,S) = \sum_{i=1}^{4}\beta_i^n = PV_{n-1} - QV_{n-2} + RV_{n-3} - SV_{n-4}$$

Given this assumption, it can be shown that

$$V_{n+1}(P,Q,R,S) = \sum_{i=1}^{4}\beta_i^{n+1}$$
$$= \sum_{i=1}^{4}\beta_i\sum_{i=1}^{4}\beta_i^n - \sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\beta_i\beta_j\sum_{i=1}^{4}\beta_i^{n-1} + \sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\beta_i\beta_j\beta_k\sum_{i=1}^{4}\beta_i^{n-2} -$$
$$\prod_{i=1}^{4}\beta_i\sum_{i=1}^{4}\beta_i^{n-3}$$
$$= PV_n - QV_{n-1} + RV_{n-2} - SV_{n-3}$$

*Sixth Order Lucas Sequence*

By analogy with the Lucas sequence, we consider the Sextic polynomial

$x^6 - b_1x^5 + b_2x^4 - b_3x^3 + b_4x^2 - b_5x + b_6 = 0$

with integer coefficients $b_1$, $b_2$, $b_3$, $b_4$, $b_5$ and $b_6$, and roots $\alpha_1$, $\alpha_2$, $\alpha_3$, $\alpha_4$, $\alpha_5$, $\alpha_6$;

where $b_1 = \sum_{i=1}^{6} \alpha_i$, $b_2 = \sum_{i=1}^{5}\sum_{j=2}^{6} \alpha_i\alpha_j$ for $i<j$, $b_3 = \sum_{i=1}^{4}\sum_{j=2}^{5}\sum_{k=3}^{6} \alpha_i\alpha_j\alpha_k$ for $i<j<k$,

$b_4 = \sum_{i=1}^{3}\sum_{j=2}^{4}\sum_{k=3}^{5}\sum_{l=4}^{6} \alpha_i\alpha_j\alpha_k\alpha_l$ for $i<j<k<l$, $b_5 = \sum_{i=1}^{2}\sum_{j=2}^{3}\sum_{k=3}^{4}\sum_{l=4}^{5}\sum_{m=5}^{6} \alpha_i\alpha_j\alpha_k\alpha_l\alpha_m$

for $i<j<k<l<m$, and $b_6 = \prod_{i=1}^{6} \alpha_i$ .

**Proposition 2:** $V_n(b_1,b_2,b_3,b_4,b_5,b_6) = \sum_{i=1}^{6} \alpha_i^{\,n}$ Let with initial values, $V_0(b_1,b_2,b_3,b_4,b_5,b_6)=6$, $V1(b_1,b_2,b_3,b_4,b_5,b_6)=b_1$, ;$V2(b_1,b_2,b_3,b_4,b_5,b_6)=b_1^{\,2}$ ; $V_3(b_1,b_2,b_3,b_4,b_5,b_6)=b_1^{\,3}-3b_1b_2+3b_3$, $V_4(b_1,b_2,b_3,b_4,b_5,b_6)=b_1^{\,4}-4b_1^{\,2}b_2+2b_2^{\,2}+4b_1b_3-4b_4$ and $V_5(b_1,b_2,b_3,b_4,b_5,b_6)=b_1^{\,5}-5b_1^{\,3}b_2+5b_1b^2+5b_1^{\,2}b_3-5b_2b_3-5b_1b_4+5b_5$.

Then, the sixth order Lucas sequence is

$$V_n(b_1,b_2,b_3,b_4,b_5,b_6) = b_1V_{n-1} - b_2V_{n-2} + b_3V_{n-3} - b_4V_{n-4} + b_5V_{n-5} - b_6V_{n-6}, \text{ for } n > 6$$

**Proof**

The Principle of Mathematical Induction is used to to prove the above. First, it must be established that $V_6$ is true

$$\begin{aligned} V_6 &= \sum_{i=1}^{6} \alpha_i^{\,6} \\ &= \sum_{i=1}^{6} \alpha_i \sum_{i=1}^{6} \alpha_i^{\,5} - \sum_{i=1}^{5}\sum_{j=2;i<j}^{6} \alpha_i\alpha_j \sum_{i=1}^{6} \alpha_i^{\,4} + \sum_{i=1}^{4}\sum_{j=2;i<j<k}^{5}\sum_{k=3;i,j<k}^{6} \alpha_i\alpha_j\alpha_k \sum_{i=1}^{6} \alpha_i^{\,3} - \\ &\quad \sum_{i=1}^{3}\sum_{j=2;i<j<k,l}^{4}\sum_{k=3;i,j<k<l}^{5}\sum_{l=4;i,j,k<l}^{6} \alpha_i\alpha_j\alpha_k\alpha_l \sum_{i=1}^{6} \alpha_i^{\,2} + \\ &\quad \sum_{i=1}^{2}\sum_{j=2;i<j<k,l,m}^{3}\sum_{k=3;i,j<k<l,m}^{4}\sum_{l=4;i,j,k<l<m}^{5}\sum_{m=5;i,j,k,l<m}^{6} \alpha_i\alpha_j\alpha_k\alpha_l\alpha_m \sum_{i=1}^{6} \alpha_i - 6\prod_{i=1}^{6} \alpha_i \\ &= b_1V_5 - b_2V_4 + b_3V_3 - b_4V_2 + b_5V_1 - b_6V_0 \end{aligned}$$

Then supposing

$$V_n(b_1,b_2,b_3,b_4,b_5,b_6) = \sum_{i=1}^{6} \alpha_i{}^n$$
$$= b_1 V_{n-1} - b_2 V_{n-2} + b_3 V_{n-3} - b_4 V_{n-4} + b_5 V_{n-5} - b_6 V_{n-6}$$

Given this assumption, it can be shown that

$$V_{n+1} = \sum_{i=1}^{6} \alpha_i{}^{n+1}$$
$$= \sum_{i=1}^{6} \alpha_i \sum_{i=1}^{6} \alpha_i{}^n - \sum_{i=1}^{5} \sum_{j=2;i<j}^{6} \alpha_i \alpha_j \sum_{i=1}^{6} \alpha_i{}^{n-1} + \sum_{i=1}^{4} \sum_{j=2;i<j<k}^{5} \sum_{k=3;i,j<k}^{6} \alpha_i \alpha_j \alpha_k \sum_{i=1}^{6} \alpha_i{}^{n-2} -$$
$$\sum_{i=1}^{3} \sum_{j=2;i<j<k,l}^{4} \sum_{k=3;i,j<k<l}^{5} \sum_{l=4;i,j,k<l}^{6} \alpha_i \alpha_j \alpha_k \alpha_l \sum_{i=1}^{6} \alpha_i{}^{n-3} +$$
$$\sum_{i=1}^{2} \sum_{j=2;i<j<k,l,m}^{3} \sum_{k=3;i,j<k<l,m}^{4} \sum_{l=4;i,j,k<l<m}^{5} \sum_{m=5;i,j,k,l<m}^{6} \alpha_i \alpha_j \alpha_k \alpha_l \alpha_m \sum_{i=1}^{6} \alpha_i{}^{n-4} - \prod_{i=1}^{6} \alpha_i \sum_{i=1}^{6} \alpha_i{}^{n-5}$$
$$= b_1 V_n - b_2 V_{n-1} + b_3 V_{n-2} - b_4 V_{n-3} + b_5 V_{n-4} - b_6 V_{n-5}$$

## THE EULER TOTIENT FUNCTION

The Lehmer totient function, *S(N)*, is the generalization of the Euler totient function for the Lucas function. In the case of the fourth order linear recurrence sequence, an analogue of this function can be constructed. In order to extend this theory, the value of the constant coefficient of the quartic equation is restricted to 1. Suppose that *N* is a positive integer, written in its canonical form, $N = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$, where the $p_i$ are distinct primes and the bi are positive integers.

Theorem 1: Let $N = p_1^{b_1} p_2^{b_2} \Lambda\ p_r^{b_r}$ where the $p_i$ are distinct primes, and $b_i$ are positive integers, and let $f(x) = x^4 - Px^3 + Qx^2 - Rx + S$ be the characteristic polynomial of the recurrence sequence $V_n = PV_{n-1} - QV_{n-2} + RV_{n-3} - SV_{n-4}$.

Euler totient function is defined as:

$$\Phi(N) = p_1^{b_1-1}\ \overline{p_1}\, p_2^{b_2-1}\ \overline{p_2} \wedge\ p_r^{b_r-1}\ \overline{p_r}$$

where

$$\overline{p_i} = \begin{cases} p_i^3 + p_i^2 + p_i + 1 & \text{if } f(x) \text{ is of type } t[4] \text{ modulo } p_i \\ p_i^3 - 1 & \text{if } f(x) \text{ is of type } t[3,1] \text{ modulo } p_i \\ p_i^2 - 1 & \text{if } f(x) \text{ is of type } t[2,1] \text{ modulo } p_i \\ p_i + 1 & \text{if } f(x) \text{ is of type } t[2] \text{ modulo } p_i \\ p_i - 1 & \text{if } f(x) \text{ is of type } t[1] \text{ modulo } p_i \end{cases}$$

Since $V_{kp_i^{b_i-1}\overline{p_i}+1} \equiv P \bmod p_i^{b_i}$ for each $i = 1, 2, \ldots, r$ and any integer $k$, we have $V_{kF(N)+1} \equiv P \bmod N$ which implies that $V_{kF(N)+1} = P \bmod N$.

Theorem 2 : Let $N = p_1^{b_1} p_2^{b_2} \Lambda\ p_r^{b_r}$ where the $p_i$ are distinct primes and $b_i$ are positive integers, and let $f(x)=x^4 + Px^3 + Qx^2 - Rx + 1$ be the characteristic polynomial of the recurrence sequence $V_n=V_n(P,Q,R,1)$. Then $V_{kF(N)+l} \equiv V_l \bmod N$ and, in particular,

$$V_{k\,F(N)+1}(P,Q,R,1) \equiv P \bmod N,$$

where $F(N)$ is Euler totient function defined above.

**Proof**

If the quartic $f(x)$ is of type $t[4]$ modulo $p_i$ and $\alpha$ is one of its roots in its splitting field over $\mathbf{F}_{pi}$, then for any positive integer $k$,

$$\beta^{kp_i^{b_i-1}(p_i^3+p_i^2+p_i+1)} \equiv S^{kp_i^{b_i-1}} \equiv 1 \bmod p_i^{b_i}$$

Therefore,

$$V_{kp_i^{b_i-1}(p_i^3+p_i^2+p+1)+1}(P,Q,R,S) \bmod p_i^{b_i} \equiv \sum_{j=1}^{4} \beta_j^{kp_i^{b_i-1}(p_i^3+p_i^2+p+1)+1} \bmod p_i^{b_i}$$

$$\equiv S^{kp_i^{b_i-1}} \sum_{j=1}^{4} \beta_j \equiv \sum_{j=1}^{4} \beta_j \equiv P \bmod p_i^{b_i}, \quad \text{if } S = 1$$

Similar for a quartic of type $t[3,1]$, $t[2,1]$, $t[2]$ and $t[1]$ modulo $p_i$.

## COMPOSITION AND INVERSE OF RECURRENCE

In this section, some properties of the sequence $V_n$, which are a direct consequence of the definition, are investigated. The rules of the composition of power and the inverse for the fourth order function are of particular importance in the process of decryption.

*Composition of Recurrences*

If the Quartic polynomial, $x^4 - P_n x^3 + Q_n x^2 - R_n x + S_n = 0$ has root has roots $\beta_1^n, \beta_2^n, \beta_3^n$ and $\beta_4^n$, then we have

i. $P_n = \sum_{i=1}^{4} \beta_i^n$

ii. $Q_n = \sum_{i=1}^{3} \sum_{j=2; i<j}^{4} \left(\beta_i \beta_j\right)^n$

iii. $R_n = \sum_{i=1}^{2} \sum_{j=2; i<j<k}^{3} \sum_{k=3; i,j<k}^{4} \left(\beta_i \beta_j \beta_k\right)^n$, and

iv. $Sn = \prod_{i=1}^{4} \beta_i^n$

Therefore, albeit is possible to get the formula $P_n$, $Q_n$, $R_n$, and $S_n$ in Lucas Sequence format, where $P$, $Q$, $R$, and $S$ are coefficients for the Quartic polynomial $x^4$-$Px^3$+$Qx^2$-$Rx$+$S$=$0$.

**Proposition 3:**

Let the quartic polynomial, $x^4$-$P_n x^3$+$Q_n x^2$-$R_n x$+$S_n$=$0$ . Then,

1. $P_n = V_n(P, Q, R, S)$, for $k \geq 4$;
2. $Q_n = V_n(Q, PR - S, P^2 S + R^2 - 2QS, PRS - S^2, QS^2, S^3)$, for $n \geq 6$;
3. $R_n = V_n(R, QS, PS^2, S^3)$, for $n \geq 4$;
4. $S_n = S^n$

where $P$, $Q$, $R$, and $S$ are coefficients for the quartic polynomial $x^4 - Px^3 + Qx^2 - Rx + S = 0$ .

**Proof**

$$P_n = \sum_{i=1}^{4} \beta_i^{\,n} = V_n(P, Q, R, S).$$

$$Q_n = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \left(\beta_i \beta_j\right)^n$$
$$= V_n(Q, PR - S, P^2S + R^2 - 2QS, PRS - S^2, QS^2, S^3), \quad \text{for } n \geq 6.$$

with initial values $Q_0 = 6; Q_1 = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \beta_i \beta_j = Q; ; Q_2 = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \left(\beta_i \beta_j\right)^2 = Q^2 - 2PR + 2S;$

$$Q_3 = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \left(\beta_i \beta_j\right)^3 = Q^3 - 3PQR - 3QS + 3P^2S + 3R^2;$$

$$Q_4 = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \left(\beta_i \beta_j\right)^4 = Q^4 - 4PQ^2R - 4Q^2S + 4P^2QS + 4R^2Q + 2P^2R^2 - 8PRS + 6S^2;$$

$$Q_5 = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \left(\beta_i \beta_j\right)^5$$
$$= Q^5 - 5PQ^3R - 5Q^3S + 5P^2Q^2S + 5R^2Q^2 + 5P^2R^2Q - 5PQRS + 5QS^2 +$$
$$5P^2S^2 + 5R^2S - 5PR^3 - 5P^3RS.$$

The Principle of Mathematical Induction is used to prove the above. First, it must be established that $Q_6$ is true.

$$Q_6 = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \left(\beta_i \beta_j\right)^6$$
$$= Q^6 - 6PQ^4R - 6Q^4S + 6P^2Q^3S + 6Q^3R^2 + 9P^2Q^2R^2 + 9Q^2S^2 - 12P^3QRS -$$
$$12PQR^3 - 2P^3R^3 + 18P^2R^2S - 18PRS^2 + 2S^3 + 3P^4S^2 + 3R^4$$
$$= QQ_5 - (PR - S)Q_4 + (P^2S + R^2 - 2QS)Q_3 - (PRS - S^2)Q_2 + (QS^2)Q_1 - (S^3)Q_0$$
$$= V_6(Q, PR - S, P^2S + R^2 - 2QS, PRS - S^2, QS^2, S^3)$$

Then, supposing

$$Q_n = \sum_{i=1}^{3} \sum_{j=2;\, i<j}^{4} \left(\beta_i \beta_j\right)^n$$
$$= (Q)Q_{n-1} - (PR - S)Q_{n-2} + (P^2S + R^2 - 2QS)Q_{n-3} - (PRS - S^2)Q_{n-4} + (QS^2)Q_{n-5} - (S^3)Q_{n-6}.$$

It can be shown that

$$
\begin{aligned}
Q_{n+1} &= \sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{n+1} \\
&= \sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\beta_i\beta_j\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta\right)_j^{\,n} - \left(\sum_{i=1}^{4}\beta_i^{\,n}\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^n - \prod_{i=1}^{4}\beta_i^{\,n}\right)\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{n-1} + \\
&\quad \left(\left(\sum_{i=1}^{4}\beta_i^{\,n}\right)^2\prod_{i=1}^{4}\beta_i^{\,n} + \left(\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^n\right)^2 - 2\prod_{i=1}^{4}\beta_i^{\,n}\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\beta_i\beta_j\right)\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{n-2} - \\
&\quad \left(\sum_{i=1}^{4}\beta_i^{\,n}\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^n\prod_{i=1}^{4}\beta_i^{\,n} - \left(\prod_{i=1}^{4}\beta_i^{\,n}\right)^2\right)\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{n-3} + \\
&\quad \left(\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\beta_i\beta_j\left(\prod_{i=1}^{4}\beta_i^{\,n}\right)^2\right)\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{n-4} - \left(\prod_{i=1}^{4}\beta_i^{\,n}\right)^3\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{n-5} \\
&= QQ_n - (PR-S)Q_{n-1} + (P^2S+R^2-2QS)Q_{n-2} - (PRS-S^2)Q_{n-3} + (QS^2)Q_{n-4} - (S^3)Q_{n-5} \\
&= V_{n+1}(Q, PR-S, P^2S+R^2-2QS, PRS-S^2, QS^2, S^3)
\end{aligned}
$$

$$
R_n = \sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^n = V_n(R, QS, PS^2, S^3), \quad \text{for } n \geq 4.
$$

with initial values $R_0 = 4; R_1 = \sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\beta_i\beta_j\beta_k = R$

The Principle of Mathematical Induction is used to prove the above. First, it must be established that $R_4$ is true.

$$
\begin{aligned}
R_4 &= \sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^4 \\
&= R(R^3 - 3QRS + 3PS^3) - QS(R^2 - 2QS) + (PS^2)R - (S^3)4 \\
&= V_4(R, QS, PS^2, S^3)
\end{aligned}
$$

Then, supposing $R_n = RR_{n-1} - QSR_{n-2} + PS^2R_{n-3} - S^3R_{n-4}$. It is shown that

$$
\begin{aligned}
R_{n+1} &= \sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^{n+1} \\
&= \sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\beta_i\beta_j\beta_k\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^n - \\
&\quad \sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\beta_i\beta_j\prod_{i=1}^{4}\beta_i^{\,n}\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^{n-1} + \\
&\quad \sum_{i=1}^{4}\beta_i^{\,n}\left(\prod_{i=1}^{4}\beta_i^{\,n}\right)^2\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta\right)_k^{n-2} - \left(\prod_{i=1}^{4}\beta_i^{\,n}\right)^3\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^{n-3} \\
&= RR_n - QSR_{n-1} + PS^2R_{n-2} - S^3R_{n-3} \\
&= V_n(R, QS, PS^2, S^3).
\end{aligned}
$$

**Proposition 4**

i. Let $V_{ed}(P,Q,R,S)=\sum_{i=1}^{4}\beta_i^{ed}$, then $V_{ed}(P,Q,R,S)=V_e(P_d,Q_d,R_d,S_d)$

ii. Let $V_{ed}(Q,PR-S,P^2S+R^2-2QS,PRS-S^2,QS^2,S^3)=\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{ed}$,

then $V_{ed}(Q,PR-S,P^2S+R^2-2QS,PRS-S^2,QS^2,S^3)$

$=V_e(Q_d,P_dR_d-S_d,P_d^2S_d+R_d^2-2Q_dS_d,P_dR_dS_d-S_d^2,Q_dS_d^2,S_d^3)$

iii. Let $V_{ed}(R,QS,PS^2,S^3)=\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^{ed}$,

then $V_{ed}(R,QS,PS^2,S^3)=V_e(R_e,Q_eS_e,P_eS_e^2,S_e^3)$

where

$P_d=V_d(P,Q,R,S)$;

$Q_d=V_d(Q,PR-S,P^2+R^2-2QS,PRS-S^2,QS^2,S^3)$;

$R_d=V_d(R,QS,PS^2,S^3)$;

$S_d=S^d$.

**Proof**

Let $\beta_1,\beta_2,\beta_3$ and $\beta_4$ be the roots of the polynomial $x^4 - Px^3 + Qx^2 - Rx + S = 0$ and $\beta_1^{\,d}$ $\beta_2,^d\beta_3^{\,d}$ and $\beta_4^{\,d}$ be the roots of the polynomial $x^4 - P_d x^3 + Q_d x^2 - R_d x + S_d = 0$.

$$V_e(P_d,Q_d,R_d,S_d)=\sum_{i=1}^{4}\left(\beta_i^{\,d}\right)^e=\sum_{i=1}^{4}\beta_i^{ed}$$
$$=V_{ed}(P,Q,R,S)$$

$$V_e(Q_d,P_dR_d-S_d,P_d^2S_d+R_d^2-2Q_dS_d,P_dR_dS_d-S_d^2,Q_dS_d^2,S_d^3)$$
$$=\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i^{\,d}\beta_j^{\,d}\right)^e=\sum_{i=1}^{3}\sum_{j=2;i<j}^{4}\left(\beta_i\beta_j\right)^{ed}$$
$$=V_{ed}(Q,PR-S,P^2S+R^2-2QS,PRS-S^2,QS^2,S^3)$$

$$V_e(R_d,Q_dS_d,P_dS_d^2,S_d^3)=\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i^{\,d}\beta_j^{\,d}\beta_k^{\,d}\right)^e=\sum_{i=1}^{2}\sum_{j=2;i<j<k}^{3}\sum_{k=3;i,j<k}^{4}\left(\beta_i\beta_j\beta_k\right)^{ed}$$
$$=V_{ed}(R,QS,PS^2,S^3)$$

*Inverse of Recurrences*

From the composition of recurrences, an inverse operation can be formulated. Consider the sequence $V_n(P,Q,R,S)$ and suppose $ed \equiv 1 \bmod \Phi(N)$, that is $ed \equiv 1 \bmod k\mathbb{F}(N) + 1$ for some integer $k$. Then, by proposition 4 and theorem 2,

$V_d(V_e(P,Q,R,1), V_e(Q,, PR\text{-}1, P^2+R^2\text{-}2Q, PR\text{-}1, Q, 1), V_e(R, Q, P, 1), 1)$
$= V_{ed}(P, Q, R, 1)$
$= V_{k\mathbb{F}(N)+1}(P, Q, R, 1)$
$\equiv P \bmod N$

$$V_d(Q_e, P_eR_e - 1, P_e^2 + R_e^2 - 2Q_e, P_eR_e - 1, Q_e, 1)$$
$$= V_{ed}(Q, PR - 1, P^2 + R^2 - 2Q, PR - 1, Q, 1)$$
$$= V_{k\Phi(N)+1}(Q, PR - 1, P^2 + R^2 - 2Q, PR - 1, Q, 1)$$
$$\equiv Q \bmod N$$

where,

$$P_e = V_e(P, Q, R, 1);$$

$$Q_e = V_e(Q, PR - 1, P^2 + R^2 - 2Q, PR - 1, Q, 1);$$

$$R_e = V_e(R, Q, P, 1).$$

$V_d(V_e(R,Q,P,1), V_e(Q, PR\text{-}1, P^2+R^2\text{-}2Q,, PR\text{-}1, Q,, 1), V_e(P, Q, R, 1), 1)$
$= V_{ed}(R, Q, P, 1)$
$= V_{k\mathbb{F}(N)+1}(R, Q, P, 1)$
$\equiv R \bmod N$

There is an obvious difference between Euler's function, $\phi(n)$, and its extension, $\mathbb{F}(n)$. The function, $\phi(n)$, depends only on the prime factors of $n$, whereas the function, $\mathbb{F}(n)$, also depends on the type of the characteristic polynomial $f(x)$. If each $\overline{p_i}$ is respectively replaced in the definition of $\mathbb{F}(n)$ by $\operatorname{lcm}(p_i^3 + p_i^2 + p_i + 1,\ p_i^3 - 1,\ p_i^2 - 1,\ p_i + 1,\ p_i - 1)$. The result is a uniform 'Totient' function, $R(N)$, which works in each case and allows the doing away with determining the type of the polynomial. The drawback is that the function is generally larger and, in the interests of computational efficiency, it is desirable to avoid moduli which are larger than necessary.

For quadratics $f(x) = x^2 - Px + 1$, the additional information needed to compute $S(N)$ is the set of Legendre symbols $\left(\frac{D}{p}\right)$, where $D = P^2 - 4$ is the discriminant of the quadratic and $p$ runs through the prime factors of N. In discussing LUC, the inverse relation involves the quantity $V_d(V_e(P, 1), 1)$ which comes from the recurrence associated

with the quadratic $g(x) = x^2 - V_e(P, 1)x + 1$ with discriminant $V_e(P, 1)^2-4$. However, $\left(\frac{P^2-4}{p}\right)=\left(\frac{V_e{}^2-4}{p}\right)$, so the type of the polynomial $g(x)$ is the same as the type of $f(x)$ and it can be found directly from the cipher $V_e(P, 1)$ without decryption.

The extension of this phenomenon to the cubic polynomial $f(x) = x_3 - Px^2 + Qx - 1$, and the argument $C_1 = V_e(P, Q, 1)$ and $C_2 = V_e(Q, P, 1)$. So, the type of the polynomial $g(x) = x^3-C_1x^2 + C_2x - 1$ is in any way related to the type of the polynomial $f(x) = x^3 - Px^2 + Qx - 1$.

In investigating the extension of the quartic polynomial, $f(x) = x^4 - Px^3 + Qx^2 - Rx + 1$; that is, given $P$, $Q$, $R$ and the argument

$C_1 = V_e(P, Q, R, 1)$,

$C_2 = V_e(Q, PR-1, P^2 + R^2 - 2Q, PR-1, Q, 1)$ and

$C_3 = V_e(R, Q, P, 1)$, a major objective is to determine whether polynomials of the type

$g(x) = x^4 - C_1x^3 + C_2x^2 - C_3x + 1$ are in any way related to polynomials of the type $f(x) = x^4-Px^3 + Qx^2-Rx + 1$.

## AN ALGORITHM TO COMPUTE THE TYPE OF QUARTIC POLYNOMIAL

It is already known that the quartic polynomial can be factorized to five major types, which are $t[4]$, $t[3,1]$, $t[2,1]$, $t[2]$ and $t[1]$. An investigation into the algorithm for computing the type of quartic polynomial in $\mathbf{F}p[x]$ follows with $p$ a prime number.

An algorithm is sketched in the form of a decision tree to compute the type of a quartic polynomial $f(x) = x^4 - Px^3 + Qx^2 - Rx + S$ in F$p[x]$, where $p$ is any prime number.

Step 1

From Quartic Equation [Weisstein,1999], the polynomial $x^4 - Px^3 + Qx^2 - Rx + S = 0$ can be modified to

$$y^2 + \frac{1}{2}(P \pm \sqrt{P^2 - 4R + 4z_1})y + \frac{1}{2}(z_1 \mu \sqrt{z_1{}^2 - 4S}) = 0.$$

It is known that the resolvent cubic polynomial

$$z^3 - Qz^2 + (PR - 4S)z + (4QS - R^2 - P^2S) = 0$$

can help in solving the quartic polynomial.

Then,

$$y^2+\tfrac{1}{2}(P\pm\sqrt{P^2-4R+4z_1})y=\tfrac{1}{2}(z_1\pm\sqrt{z_1{}^2-4S})$$

$$\left(y+\tfrac{1}{4}(P\pm\sqrt{P^2-4R+4z_1})\right)^2=\left(\tfrac{1}{4}(P\pm\sqrt{P^2-4R+4z_1})\right)^2+\tfrac{1}{2}(z_1\pm\sqrt{z_1{}^2-4S})$$

$$\left(256y+64(P\pm\sqrt{P^2-4R+4z_1})\right)^2=\left(P\pm\sqrt{P^2-4R+4z_1}\right)^2+8(z_1\pm\sqrt{z_1{}^2-4S})$$

For this case, the roots are integers modulo $p$. So, this equation modulo $p$ can be used. Thus,

$$\left(256y+64(P\pm\sqrt{P^2-4R+4z_1})\right)^2$$

$$\equiv\left(P\pm\sqrt{P^2-4R+4z_1}\right)^2+8(z_1\pm\sqrt{z_1{}^2-4S})\bmod p$$

Step 2A

$f$ is of type $t[4]$, if and only if $P^2-4R+4z_1$ or $z_1{}^2-4S \bmod p$ are not perfect squares; or there is no real root in the resolvent cubic polynomial.

It is already known that no having a real root in the resolvent cubic polynomial results in the inability to solve the quartic polynomial. And, if $P^2-4R+4z_1$ or $z_1{}^2-4S \bmod p$ is not a perfect square, the problem cannot be solved also.

Step 2B

If there is at least a real roots in the resolvent cubic polynomial; and $P^2-4R+4z_1$, and $z_1{}^2-4S \bmod p$ are perfect squares, there will exist three types for quartic polynomials.

$f$ is of type $t[2]$, if and only if $\left(\frac{\left(P\pm\sqrt{P^2-4R+4z_1}\right)^2+8(z_1\pm\sqrt{z_1{}^2-4S})}{p}\right)\neq 1$

$f$ is of type $t[2,1]$, if and only if $\left(\frac{\left(P+\sqrt{P^2-4R+4z_1}\right)^2+8(z_1+\sqrt{z_1{}^2-4S})}{p}\right)\neq\left(\frac{\left(P-\sqrt{P^2-4R+4z_1}\right)^2+8(z_1-\sqrt{z_1{}^2-4S})}{p}\right)$

$f$ is of type t[1], if and only if $\left(\frac{\left(P\pm\sqrt{P^2-4R+4z_1}\right)^2+8(z_1\pm\sqrt{z_1{}^2-4S})}{p}\right)=1$

Step 2C

If there is a real root in the resolvent Cubic polynomial, then it is of case *t*[2], *t*[2,1] or *t*[1]. If there is no real root in the Resolvent Cubic polynomial, then it is of case *t*[4]. Thus, there is no condition for type *t*[3,1]. However, Stickelberger's theorem [5] is used here to compute the Quartic polynomial of type *t*[3,1]. At the same time, there is a need for another condition to compute it.

**Theorem 3 (Stickelberger's Theorem)**

Let *p* an odd prime *f*(*x*) be a monic polynomial of degree *d* with coefficients in $\mathbf{F}p[x]$ without multiple factors. Let *r* be the number of irreducible factors of *f*(*x*) in $\mathbf{F}_p[x]$.

Then r≡d mod 2 and only if $\left(\frac{D}{p}\right)=1$.

From theorem 3, it is known that if the Quartic polynomial is of type t[3,1], $\left(\frac{D}{p}\right)=-1$ .

But, this condition also fulfills for another type, like t[1]. Therefore, it must be ensured that there is at least a condition for type *t*[1] that is not fulfilled.

## THE QUARTIC CRYPTOSYSTEM

As in the RSA, LUC and $LUC_3$ cryptosystems, the strength of the system to be constructed depends on the difficulty of factoring large numbers. Thus, it is necessary to pick two large secret primes *p* and q, the product of *N* which is part of the encryption key. The encryption key is (*e, N*) which is made public. Note that, *e* must be chosen so that it is relatively prime to the function $\Phi(N)=\overline{pq}$ because it is necessary to solve the congruence $ed\equiv 1 \bmod \Phi(N)$ to find the decoding key *d*. In practice, since $\Phi(N)$ depends on the type of an auxiliary polynomial, we choose *e* prime to *p*-1, *q*-1 ,*p*+1, *q*+1, $p^2$-1, $q^2$-1, $p^3$-1, $q^3$+1, $p^3+p^2+p+1$,$q^3+q^2+q+1$ to cover all possible cases.

With these preliminary observations, a public-key cryptosystem will be set out based on the quartic recurrence sequence $V_n$ derived from the quartic polynomial, $x^4-Px^3+Qx^2-Rx+S=0.$

The encryption function is defined by

$$E(P,Q,R)=(V_e(P,Q,R,1),V_e(Q,PR-1,P^2+R^2-2Q,PR-1,Q,1),V_e(R,Q,P,1))$$
$$\equiv(C_1,C_2,C_3)\bmod N$$

where *N*=*pq* as above, (*P*,*Q*,*R*) constitutes the message and the encryption key, (*e*,*N*). $V_e(P,Q,R,1)$ and $V_e(R,Q,P,1)$ are the *e*-th term of the quartic recurrence and $Ve(Q,PR-1,P^2+R^2-2Q,PR-1,Q,1)$ is *e*-th term of the Sextic recurrence defined earlier.

The decryption key is $(d, N)$ where $d$ is the inverse of $e$ modulo $\mathrm{F}(N)$. To decipher the message, the receiver must know or be able to compute $\mathrm{F}(N)$ and then calculate

$$D(C_1, C_2, C_3)$$
$$= (V_d(C_1, C_2, C_3, 1), V_d(C_2, C_1C_3 - 1, C_1^2 + C_3^2 - 2C_2, C_1C_3 - 1, C_2, 1), V_d(C_3, C_2, C_1, 1))$$
$$\equiv (P, Q, R) \bmod N$$

which recovers the original message $(P,Q,R)$.

In decryption, $g(x) = x^4 - C_1x^3 + C_2x^2 - C_3x + 1$, is given but not $f(x) = x^4 - Px^3 + Qx^2 - Rx + 1$ and so we have to deduce the type of $f$ in order to apply the algorithm correctly.

Example

The following example is an illustration that describes the details required in the computations to show how the system works.

Let $p$=23 and $q$=29 be two primes and thus $N$=667. Assume that the plain text messages are $P$=17, $Q$=7, $R$=21. The function $f$ is given by $f(x) = x^4 - 17x^3 + 7x^2 - 21x + 1.$ If the encryption key is $e$=41, then the sender calculates

$$C_1 = V_e(P, Q, R, 1) = V_{41}(17, 7, 21, 1)$$
$$\equiv 108 \bmod 667$$

$$C_2 = V_e(Q, PR - 1, P^2 + R^2 - 2Q, PR - 1, Q, 1) = V_{41}(7, 356, 716, 356, 7, 1)$$
$$\equiv 558 \bmod 667$$

$$C_3 = V_e(R, Q, P, 1) = V_{41}(21, 7, 17, 1)$$
$$\equiv 249 \bmod 667$$

$$E(P, Q, R) \equiv (C_1, C_2, C_3) \bmod N$$
$$\equiv (108, 558, 249) \bmod 667$$

The receiver thus constructs the function $g(x)=x^4-108x^3+558x^2-249x+1$. In order to determine the decryption key $d$, the owner of the encryption key $(41,667)$ has to determine the function $\Phi(N)$ and, to this end, must deduce the type of the function $f$ with respect to the primes $p$ and $q$.

For prime $p$=23, discriminant of $g$ is $D \equiv 9 \bmod 23$ which is non-zero and this implies that $f$ is of the same type as $g$, namely $t[1,1,1,1]$ since the function

$$\begin{aligned} g(x) &= x^4 - 108x^3 + 558x^2 - 249x + 1 \\ &\equiv x^4 + 7x^3 + 6x^2 + 4x + 1 \bmod 23 \\ &\equiv (x+13)(x+9)(x+6)(x+2) \bmod 23 \end{aligned}$$

(In fact,

$$\begin{aligned} f(x) &= x^4 - 17x^3 + 7x^2 - 21x + 1 \\ &\equiv x^4 + 6x^3 + 7x^2 + 2x + 1 \bmod 23 \\ &\equiv (x+13)(x+9)(x+4)(x+3) \bmod 23.) \end{aligned}$$

In case of the primes $q$ =29 , discriminant of $g$ is $D \equiv 28$ and 29 which is non-zero and this implies that $f$ is of the same type as $g$, namely $t[1,1,1,1]$, since the function

$$\begin{aligned} g(x) &= x^4 - 108x^3 + 558x^2 - 249x + 1 \\ &\equiv x^4 + 8x^3 + 7x^2 + 12x + 1 \bmod 29 \\ &\equiv (x+28)(x+19)(x+10)(x+9) \bmod 29 \end{aligned}$$

(In fact,

$$\begin{aligned} f(x) &= x^4 - 17x^3 + 7x^2 - 21x + 1 \\ &\equiv x^4 + 12x^3 + 7x^2 + 8x + 1 \bmod 29 \\ &\equiv (x+28)(x+26)(x+13)(x+3) \bmod 29.) \end{aligned}$$

Therefore,

$$\Phi(N) = \Phi(23 \bullet 29) = (23-1)(29-1) = 616$$

and, the decryption key

$$\begin{aligned} ed &\equiv 1 \bmod \Phi(N) \\ 41d &\equiv 1 \bmod 616 \\ d &\equiv 41^{-1} \bmod 616 \\ &\equiv 601 \bmod 616 \end{aligned}$$

Now, the receiver can readily decrypt by computing

$$\begin{aligned} P &\equiv V_d(C_1, C_2, C_3, 1) \bmod N \\ &\equiv V_{601}(108, 558, 149, 1) \bmod 667 \\ &\equiv 17 \bmod 667 \end{aligned}$$

$$\begin{aligned} Q &\equiv V_d(C_2, C_1C_3 - 1, C_1^2 + C_3^2 - 2C_2, C_1C_3 - 1, C_2, 1) \bmod N \\ &\equiv V_{601}(558, 211, 513, 211, 558, 1) \bmod 667 \\ &\equiv 7 \bmod 667 \end{aligned}$$

$$\begin{aligned} R &\equiv V_d(C_3, C_2, C_1, 1) \bmod N \\ &\equiv V_{601}(149, 558, 108, 1) \bmod 667 \\ &\equiv 21 \bmod 667 \end{aligned}$$

$$\begin{aligned} D(C_1, C_2, C_3) &\equiv (17, 7, 21) \bmod 667 \\ &\equiv (P, Q, R) \bmod N \end{aligned}$$

## THE EFFICIENCY AND SECURITY

As in the LUC cryptosystem, the first obvious test of the efficiency of the extended system is the ability to compute the *e*-th of the fourth order and sixth order Lucas sequences; they are , $V_e(P,Q,R,1)$, $V_e(R,Q,P,1)$ and $V_e(Q,PR\text{-}1,P^2+R^2\text{-}2Q,PR\text{-}1,Q,,1)$, in a reasonable amount of time, close to the efficiency of calculation the *e*-th power of an integer. Smith and Lennon (1993) claim that LUC is as efficient as RSA. Besides that, Said and Loxton (2003) claim that the efficiency of $LUC_3$ is close to the efficiency of LUC. Thus, we can assume that the efficiency of $LUC_4$ is close to the efficiency of RSA, LUC, and $LUC_3$.

The $LUC_4$ cryptosystem is analogous to the RSA cryptosystem; therefore the security for this cryptosystem is similar to the security for RSA cryptosystem. The GCD attack is one of the polynomial attacks on the RSA-type cryptosystems. If two messages differ only from a known fixed value $\Delta$ and are RSA-encrypted under same RSA-modulus *n*, then it is possible to recover both of them.

Let $(P_1,Q_1,R_1)$ be the first set of the message and $(P_2,Q_2,R_2) = (P_1+\Delta_1, Q_1+\Delta_2, R_1+\Delta_3)$ be the second set of the message and let $(C_1,C_2,C_3) \equiv E(P_1,Q_1,R_1) \bmod N$ and $(C_4,C_5,C_6) \equiv E(P_2,Q_2,R_2) \bmod N$, where $E(P_i,Q_i,R_i) \bmod N$ is encryption function defined previously. Then, form the polynomial $X_i$ and $Y_i \in Z_n[x_1, x_2, x_3]$, defined by

$$X_1(x_1, x_2, x_3) = V_e(x_1, x_2, x_3, 1) - C_1 \bmod N \ ;$$

$$X_2(x_1, x_2, x_3) = V_e(x_2, x_1x_3 - 1, x_1^2 + x_3^2 - 2x_2, x_1x_3 - 1, x_2, 1) - C_2 \bmod N \ ;$$

$$X_3(x_1,x_2,x_3) = V_e(x_3,x_2,x_1,1) - C_3 \bmod N \ ;$$

$$Y_1(x_1,x_2,x_3) = V_e(x_1,x_2,x_3,1) - C_4 \bmod N \ ;$$

$$Y_2(x_1,x_2,x_3) = V_e(x_2,x_1x_3-1,x_1^2+x_3^2-2x_2,x_1x_3-1,x_2,1) - C_5 \bmod N \ ; \text{ and}$$

$$Y_3(x_1,x_2,x_3) = V_e(x_3,x_2,x_1,1) - C_6 \bmod N$$

Since the message $(P_1,Q_1,R_1)$ are roots of the polynomial $(X_1,X_2,X_3)$ and $(Y_1,Y_2,Y_3)$ $P_1$,will be the root of $W_1=gcd(X_1,Y_1)$, $Q_1$ will be the root of $W_2=gcd(X_2,Y_2)$, and $R_1$ will be the root of $W_3=gcd(X_3,Y_3)$. Solving the polynomial $W_i$ in $x_1$, $x_2$ , and $x_3$ give the value of $(P_1,Q_1,R_1)$ and $(P_2,Q_2,R_2) = (P_1+\Delta_1, Q_1+\Delta_2, R_1+\Delta_3)$ .

According to our objective, we develop a cryptosystem which is using fourth order and sixth order linear recurrence of Lucas sequence in the process of encryption and decryption. Beside that, the composition and inverse of recurrence help us to recover the original message in the process of decryption. The Euler totient function gives us the conditions of encryption key and helps us to find the decryption key. However, the Euler totient function depends on which type of quartic polynomial. Therefore, an algorithm to compute the type has been defined. A new cryptosystem has been developed which is able to compute three messages, (*P, Q, R*) for each calculation. Some aspects of efficiency and security were discussed, but further research is needed to address these issues.

## REFERENCES


CHILDS, L. N. 1979. The discriminant and the Stickelberger's Theorem. In *A Concrete Introduction to High Algebra*, p. 282-289. New York: Springer-Verlag Press.

DIFFIE, W. and M. HELLMAN. 1976. New directions in cryptography. *IEEE Trans. Inform. Theory* **IT-22(6):** 644-654.

LEHMER, D. H. 1930. An extended theory of Lucas ' function'. *Annals of Math.* **31:** 419-448.

RIVEST, R., A. SHAMIR and L. ADLEMAN. 1978. A method for obtaining digital signatures and public key cryptosystems. *Comm. of the ACM* **21:** 120-126.

SAID, M.R.M and J. LOXTON. 2003. A cubic analogue of the RSA cryptosystem. *Bulletin of the Australia Mathematical Society* **68:** 21-38.

SMITH, P.J. and M.J.J. LENNON. 1993. LUC: A new public key system. In *Proceedings of the Ninth IFIP International Symposium on Computer Security*, p. 103-117.

WILLIAMS, H.C. 1972. On a generalization of the Lucas functions. *Acta Arithmetica* **20:** 33-51.

WILLIAMS, H.C. 1982. A p+1 method of factoring. *Mathematics of Computation* **39:** 225-234.

WEISSTEIN, E.W. 1999. *Quartic Equation.* Mathworld, Wolfram Research, Inc. *http://mathworld.wolfram.com/QuarticEquation.html*