An Approach of Cryptosystem using Polynomials and Lucas Numbers

Gudela Ashok [1*], S. Ashok Kumar [2], and D. Chaya Kumari [3]
[1]Research Scholar, Department of Mathematics, Andhra University TDR Hub & Assistant Professor,
Department of Mathematics, Adikavi Nannaya University.
[2,3] Assistant Professor, Gayatri Vidya Parishad College for Degree and P.G.Courses(A).

Abstract- This paper presents an innovative approach to a cryptosystem that utilizes polynomials and Lucas numbers. Lucas numbers, a sequence similar to Fibonacci numbers, offer unique properties that can be leveraged for encryption and decryption. The proposed Lucas Polynomial Cryptosystem outlines the key generation, encryption, and decryption processes, highlighting the security considerations and key management aspects. The system's strength relies on the difficulty of factoring large prime numbers and the challenge of deriving the secret key from the public key. This paper aims to provide a comprehensive understanding of the cryptosystem and explores its potential applications in secure communications and data protection. Extensive analysis and cryptanalysis have been conducted to evaluate the system's security and effectiveness, making it a promising addition to the cryptographic landscape.

Keywords- Cryptography, Polynomials, Lucas numbers, Lucas Polynomials

1 Introduction

In today's interconnected world, the need for secure communication and data protection has become paramount. Cryptography, the science of encrypting and decrypting information, plays a critical role in safeguarding sensitive data from unauthorized access and ensuring the confidentiality, integrity, and authenticity of digital communications. Over the years, numerous cryptographic systems and algorithms have been developed, each with its unique approach to securing information.

This paper presents an innovative and novel approach to a cryptosystem that combines the power of polynomials and Lucas numbers. Lucas numbers, a sequence closely related to the well-known Fibonacci numbers, possess distinct mathematical properties that can be harnessed for cryptographic purposes. By leveraging the characteristics of these numbers in conjunction with polynomials, we propose the "Lucas Polynomial Cryptosystem," a potentially robust and secure encryption technique.[1]-[4]

The primary goal of this paper is to explore the fundamental concepts, mechanisms, and applications of the Lucas Polynomial Cryptosystem. We will delve into the key components of the system, including key generation, encryption, and decryption processes, unravelling the mathematical intricacies that underpin its security. Additionally, we will address the essential considerations of key management to ensure the confidentiality and integrity of sensitive information.

The strength of the Lucas Polynomial Cryptosystem lies in the complexity of factorizing large prime numbers, a challenging task that forms the foundation of its security. We will discuss how the system's security is augmented by the secret key, a Lucas number, and the difficulty of deriving this key from the publicly available modulus. A thorough analysis of the system's security will be conducted, scrutinizing its resilience against potential attacks and vulnerabilities.

Throughout this paper, we aim to offer a comprehensive understanding of the Lucas Polynomial Cryptosystem, exploring its strengths, limitations, and potential applications in real-world scenarios. Cryptanalysis and security evaluations will be discussed to shed light on the system's performance and to identify areas where further improvements may be required.

In conclusion, the Lucas Polynomial Cryptosystem represents an innovative and intriguing approach to cryptographic techniques. As the digital landscape continues to evolve, cryptographic systems that are both secure and efficient become increasingly critical. By harnessing the power of polynomials and Lucas numbers, this cryptosystem opens new avenues for secure communication, data protection, and confidential information exchange. Through rigorous examination and analysis, we hope to contribute valuable insights to the realm of cryptography and pave the way for future advancements in secure information transmission.[1]-[4][20]

2 Definitions and Standard results

2.1 Cryptography

Cryptography is the science and practice of secure communication, encompassing techniques for encoding and decoding information to ensure its confidentiality, integrity, and authenticity. It involves the use of mathematical algorithms and cryptographic protocols to transform plaintext (original, readable data) into ciphertext (encoded, unreadable data) in such a way that only authorized parties with the appropriate key can decipher the ciphertext and access the original information. Cryptography plays a crucial role in securing digital data, protecting sensitive information, enabling secure transactions over the internet, and ensuring the privacy of communication in various applications, including online banking, e-commerce, messaging, and data storage.[1][2]

2.2 Plaintext

In cryptography, plaintext refers to the original, readable, and unencrypted data or message before it undergoes any cryptographic transformation. It represents the information that needs to be protected from unauthorized access or interception.

2.3 Ciphertext

Ciphertext is the encrypted and unintelligible representation of the plaintext data produced by applying cryptographic algorithms. It results from the process of encryption and serves as a secure form of the original data, making it challenging for unauthorized individuals to understand the content without the appropriate decryption key.

2.4 Encryption

Encryption is the process of converting plaintext data into ciphertext using cryptographic algorithms and keys. It ensures data confidentiality by rendering the information unreadable and incomprehensible to anyone without the corresponding decryption key.[5]

2.5 Decryption

Decryption is the reverse process of encryption, involving the transformation of ciphertext back into plaintext using the appropriate decryption key. It is performed by authorized parties to retrieve the original data from the encrypted form.[5]

2.6 Cryptanalysis

Cryptanalysis is the study and analysis of cryptographic systems to identify potential vulnerabilities and weaknesses that may allow unauthorized access to encrypted data without the decryption key. It involves various techniques, such as mathematical analysis, statistical methods, and brute force attacks, to break or compromise cryptographic algorithms.[6]

2.7 Symmetric Key Cryptography

Symmetric key cryptography, also known as secret-key cryptography, is a cryptographic approach where the same key is used for both encryption and decryption processes. The sender and receiver possess and exchange the secret key securely before communicating. While it offers fast processing, the challenge lies in securely distributing and managing the secret keys.[6]

2.8 Asymmetric Key Cryptography

Asymmetric key cryptography, also called public-key cryptography, employs a pair of mathematically related keys: a public key used for encryption and a private key used for decryption. The public key is openly distributed, while the private key is kept secret. This approach offers enhanced security and enables secure key exchange without prior communication between parties.[6]

2.9 Key Management

Key management refers to the practices and processes involved in securely generating, distributing, storing, and revoking cryptographic keys. Proper key management is essential to maintain the security and integrity of encrypted data and prevent unauthorized access to sensitive information.

2.10 Polynomial

A polynomial is a mathematical expression consisting of variables (usually represented by the letter "x") and coefficients, combined using addition, subtraction, and multiplication, but not division by variables. The variables in a polynomial can only have non-negative integer exponents. It can be represented in the general form $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$.

In this representation, *P(x)* is the polynomial function, *x* is the variable, and $a_0, a_1, a_2, \dots, a_n$ are constants called coefficients.[9]

2.11 Truncated polynomial

The truncated polynomial of order *N* is a polynomial whose degree is limited to *N*, meaning it contains only the terms up to the *N*th degree. Any terms with degrees greater than *N* are excluded, effectively "truncating" the polynomial.

A truncated polynomial of order N can be represented $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_Nx^N$

In this representation, the coefficients $a_0, a_1, a_2, \ldots, a_N$ are constants, and *x* is the variable. The highest degree of *x* in the polynomial is *N*, and any term with a degree greater than *N*, such as $a_{N+1}x^{N+1}$ *or* $a_{N+2}x^{N+2}$ *or* $a_{N+3}x^{N+3}$, is omitted.[10][11][12]

2.12 Text to binary coding

Text to binary digits conversion, also known as text to binary encoding, is the process of converting human-readable text characters into their binary representation. In this encoding, each character of the text is represented using a sequence of 0s and 1s, where each digit corresponds to a specific character according to a predefined encoding scheme, such as ASCII (American Standard Code for Information Interchange) or Unicode.[13]

For example, let's convert the word "HELO" into binary using the ASCII encoding scheme:

1. H -> ASCII value: 72 -> Binary representation: 01001000
2. E -> ASCII value: 69 -> Binary representation: 01000101
3. L -> ASCII value: 76 -> Binary representation: 01001100
4. O -> ASCII value: 79 -> Binary representation: 01001111

2.13 Lucas numbers

Lucas numbers are a sequence of integers that form a numerical series similar to the Fibonacci numbers.

$$L_n = \begin{cases} 2 & ;\text{if } n = 0 \\ 1 & ;\text{if } n = 1 \\ L_{n-1} + L_{n-2} & ;\text{if } n > 1 \end{cases}$$

The Lucas numbers are in the following integer sequence 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123,…[14][15]

2.14 Lucas Polynomial

The Locus Polynomials are defined by a recurrence relation [16][17][18]

$$L_n(x) = \begin{cases} 2 & ;\text{if } n = 0 \\ x & ;\text{if } n = 1 \\ xL_{n-1}(x) + L_{n-2}(x) & ;\text{if } n \geq 2 \end{cases}$$

3 Algorithm

Encryption algorithm steps

➢ Choose any integers *p, q, N* and multiply *p, q* to get $n = pq$, where *n* is called the modulus for encryption and decryption.

➢ Choose a random polynomial f truncated to order *N* and find inverse of f under modulo *n* that is $f_n(mod\ n)$

➢ Take the plain text '*m*'. First, convert it into its corresponding binary digits. Next, convert the binary representation into octal numbers using ASCII. Finally, we'll express each octal number as its numerical equivalent and represent them as $m = m_1, m_2, m_3, \ldots$ in the form of corresponding polynomials.

➢ The Cipher text $C_1 = m_1.f_n(mod\ n)$ and so on.

➢ By applying the offset rule of Lucas sequences or Lucas polynomials to the cipher text C_1, will generate the encrypted text C_2, which will be sent to the receiver. [19]

Encryption algorithm steps

➢ Upon receiving the encrypted text C_2 from the sender, the receiver will decrypt it using the secret key (reverse offset rule of Vieta-Pell-Lucas) and denote the decrypted message as m_1.

➢ Receiver again decrypts the message m_1' using $m_2' = f_n^{-1}m_1'(mod\ n)$.

➢ Convert m_2' to respective Octal and then binary values.

➢ Convert obtained binary into ASCII characters from which plain text '*m*' can be retrieved[19]

➢

4 Example with Lucas Numbers

Step 1: Let us choose integer *N* and two primes *p, q* that is *N=12, p=3 & q=7* and Compute $n = p \times q \Rightarrow n = 3 \times 7 \Rightarrow n = 21$

Step 2: Choose a random polynomial $f = 1 + X - X^2 + X^3 - X^5 + X^6 - X^8 - X^9 + X^{11} + X^{12}$

Step 3: Now find inverse of f under modulo *n* that is $f_n(mod\ n)$ truncated to order *N*

$$f_n(mod\ n) = 3 + 8X + 18X^2 + 12X^3 + 4X^4 + 7X^6 + 16X^7 + 7X^9 + 17X^{10} + 9X^{11} + 15X^{12}(mod\ 21)$$

And also find $f_n^{-1}(mod\ n) = f(mod\ n)$

$$f_n^{-1} = 1 + X - X^2 + X^3 - X^5 + X^6 - X^8 - X^9 + X^{11} + X^{12}(mod\ n) = f$$

Step 4: Take the plain text message "MAHID" and Convert it into its corresponding binary digits

$$M = 1001101, A = 1000001, H = 1001000\ , \mathrm{I} = 1001001 \text{ and } \mathrm{D} = 1000100$$

Now convert binary to Octal, $M = 115, A = 101, H = 110\ , \mathrm{I} = 111 \text{ and } \mathrm{D} = 104$

Again convert them into polynomials, just add an *x* to the respective powers as follows

$$I_M = 5 + X + X^2, I_A = 1 + X^2, I_H = X + X^2, I_I = 1 + X + X^2 \text{ and } I_D = 4 + X^2$$

Let us take the pain text 'MAHID' into polynomials $I_M, I_A, I_H\ , I_I, I_D$ respectively.

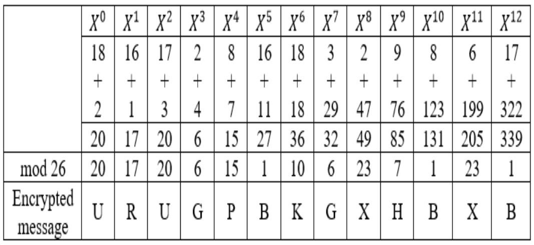
Encryption *message* of I_M

Step 5: Let the cipher text $C_1 = I_M . f_n(mod\ n)$

$$C_1 = (5 + X + X^2)(3 + 8X + 18X^2 + 12X^3 + 4X^4 + 7X^6 + 16X^7 + 7X^9 + 17X^{10} + 9X^{11} + 15X^{12})(mod\ 21)$$

$$C_1 = 18 + 16X + 17X^2 + 2X^3 + 8X^4 + 16X^5 + 18X^6 + 3X^7 + 2X^8 + 9X^9 + 8X^{10} + 6X^{11} + 17X^{12}(mod\ 21)$$

Step 6: Now apply offset rule with Lucas numbers



	X^0	X^1	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	X^{10}	X^{11}	X^{12}
	18 + 2	16 + 1	17 + 3	2 + 4	8 + 7	16 + 11	18 + 18	3 + 29	2 + 47	9 + 76	8 + 123	6 + 199	17 + 322
	20	17	20	6	15	27	36	32	49	85	131	205	339
mod 26	20	17	20	6	15	1	10	6	23	7	1	23	1
Encrypted message	U	R	U	G	P	B	K	G	X	H	B	X	B

Fig. 1. Offset rule with Lucas numbers

Encrypted message is URUGPBKGXHBXB

For the remaining characters, use the same procedure follows,

Encryption message of I_A

Consider the Cipher text be $C_1 = I_A . f_n(mod\ n)$

$$C_1 = 12 + 2X + 20X^3 + X^4 + 12X^5 + 11X^6 + 16X^7 + 7X^8 + 2X^9 + 17X^{10} + 16X^{11} + 11X^{12}(mod\ 21)$$

Apply Offset rule with Lucas numbers and then get Encrypted message is ODDYIXDTCAKHV

Encryption message of I_H

Let the Plain text be $C_1 = I_H . f_n(mod\ n)$

$$C_1 = 3 + 18X + 11X^2 + 5X^3 + 9X^4 + 16X^5 + 4X^6 + 7X^7 + 2X^8 + 16X^9 + 7X^{10} + 3X^{11} + 5X^{12}(mod\ 21)$$

Apply Offset rule with Lucas numbers and then get Encrypted message is TOJQBWKXOAUP

Encryption message of I_I

Let the Plain text be $C_1 = I_I . f_n(mod\ n)$

$$C_1 = 6 + 5X + 8X^2 + 17X^3 + 13X^4 + 16X^5 + 11X^6 + 2X^7 + 2X^8 + 2X^9 + 3X^{10} + 12X^{11} + 20X^{12}(mod\ 21)$$

Apply Offset rule with Lucas numbers and then get Encrypted message is IGLVUBDFXAWDE

Encryption message of I_D

Let the Plain text be $C_1 = I_D . f_n(mod\ n)$

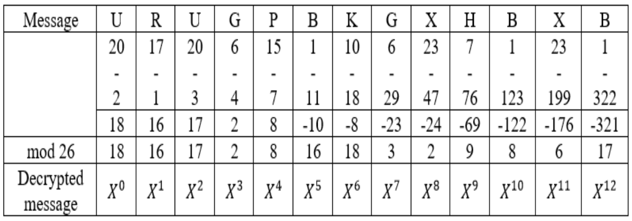
$$C_1 = 5X + 12X^2 + 14X^3 + 13X^4 + 12X^5 + 11X^6 + X^7 + 7X^8 + 2X^9 + 5X^{10} + X^{11} + 14X^{12}(mod\ 21)$$

Apply Offset rule with Lucas numbers and then get Encrypted message is GPSUXDECAYSY

Decryption message of I_M

Step 1: To get first decrypted Message take URUGPBKGXHBXB

Step 2: Now apply Reverse Offset rule with Lucas numbers for the first decrypted message



Message	U	R	U	G	P	B	K	G	X	H	B	X	B
	20 - 2	17 - 1	20 - 3	6 - 4	15 - 7	1 - 11	10 - 18	6 - 29	23 - 47	7 - 76	1 - 123	23 - 199	1 - 322
	18	16	17	2	8	-10	-8	-23	-24	-69	-122	-176	-321
mod 26	18	16	17	2	8	16	18	3	2	9	8	6	17
Decrypted message	X^0	X^1	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	X^{10}	X^{11}	X^{12}

Fig. 2. Reverse Offset rule with Lucas numbers

$$C_1 = 18 + 16X + 17X^2 + 2X^3 + 8X^4 + 16X^5 + 18X^6 + 3X^7 + 2X^8 + 9X^9 + 8X^{10} + 6X^{11} + 17X^{12}(mod\ 21)$$

Step 3: Find $I_M = f_n^{-1} C_1(mod\ n)$

$$I_M = (1 + X - X^2 + X^3 - X^5 + X^6 - X^8 - X^9 + X^{11} + X^{12})(18 + 16X + 17X^2 + 2X^3 + 8X^4 + 16X^5 + 18X^6 + 3X^7 + 2X^8 + 9X^9 + 8X^{10} + 6X^{11} + 17X^{12})(mod\ 21)$$

$$I_M = 5 + X + X^2(mod\ 21)$$

Step 4: Convert polynomial to respective OCTAL numbers representations.$5 + X + X^2 = 115$

Step 5: Convert Octal to respective binary representations.$115 = 1001101$

Step 6: Finally, Convert binary to letters, Using ASCII conversions.$1001101 = M$

For the remaining characters, use the same procedure follows,

Decryption message of I_A

To get first decrypted Message take ODDYIXDTCAKHV

Now apply Reverse Offset rule with Lucas numbers for the decrypted message

$$C_1 = 12 + 2X + 20X^3 + X^4 + 12X^5 + 11X^6 + 16X^7 + 7X^8 + 2X^9 + 17X^{10} + 16X^{11} + 11X^{12}(mod\ 21)$$

$$I_A = f_n^{-1} C_1(mod\ n) = 1 + X^2(mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters.

$1 + X^2 = 101$=1000001 $= Ab$

Decryption message of I_H

To get first decrypted Message take FTOJQBWKXOAUP

Now apply Reverse Offset rule with Lucas numbers for the decrypted message

$$C_1 = 3 + 18X + 11X^2 + 5X^3 + 9X^4 + 16X^5 + 4X^6 + 7X^7 + 2X^8 + 16X^9 + 7X^{10} + 3X^{11} + 5X^{12} (mod\ 21)$$

$$I_H = f_n^{-|} C_1 (mod\ n) = X + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters $X + X^2 = 110 = 1001000 = H$

Decryption message of I_I

To get first decrypted Message take IGLVUBDFXAWDE

Now apply Reverse Offset rule with Lucas numbers for the decrypted message

$$C_1 = 6 + 5X + 8X^2 + 17X^3 + 13X^4 + 16X^5 + 11X^6 + 2X^7 + 2X^8 + 2X^9 + 3X^{10} + 12X^{11} + 20X^{12} (mod\ 21)$$

$$I_I = f_n^{-|} C (mod\ n) = 1 + X + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters $1 + X + X^2 = 1001001 = I$

Decryption message of I_D

To get first decrypted Message take CGPSUXDECAYSY

Now apply Reverse Offset rule with Lucas numbers for the decrypted message

$$C_1 = 5X + 12X^2 + 14X^3 + 13X^4 + 12X^5 + 11X^6 + X^7 + 7X^8 + 2X^9 + 5X^{10} + X^{11} + 14X^{12} (mod\ 21)$$

$$I_D = f_n^{-|} C (mod\ n) = 4 + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters $4 + X^2 = 104 = 1000100 = D.$

5 Example with Lucas polynomials

Encryption message of I_M

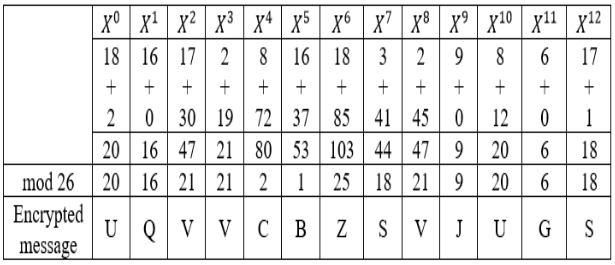
Let the cipher text $C_1 = I_M . f_n (mod\ n)$

$$C_1 = (5 + X + X^2)(3 + 8X + 18X^2 + 12X^3 + 4X^4 + 7X^6 + 16X^7 + 7X^9 + 17X^{10} + 9X^{11} + 15X^{12})(mod\ 21)$$

$$C_1 = 18 + 16X + 17X^2 + 2X^3 + 8X^4 + 16X^5 + 18X^6 + 3X^7 + 2X^8 + 9X^9 + 8X^{10} + 6X^{11} + 17X^{12} (mod\ 21)$$

Offset rule with Lucas polynomial[16]-[18]

$$L_{12}(x) = 2 + 30X^2 + 19X^3 + 72X^4 + 37X^5 + 85X^6 + 41X^7 + 45X^8 + 12X^{10} + X^{12}$$



	X^0	X^1	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	X^{10}	X^{11}	X^{12}
	18 + 2	16 + 0	17 + 30	2 + 19	8 + 72	16 + 37	18 + 85	3 + 41	2 + 45	9 + 0	8 + 12	6 + 0	17 + 1
	20	16	47	21	80	53	103	44	47	9	20	6	18
mod 26	20	16	21	21	2	1	25	18	21	9	20	6	18
Encrypted message	U	Q	V	V	C	B	Z	S	V	J	U	G	S

Fig. 3. Offset rule with Lucas polynomial

Encrypted message is UQVVCBZSVJUGS

Encryption message of I_A

Consider the Cipher text be $C_1 = I_A . f_n (mod\ n)$

$$C_1 = 12 + 2X + 20X^3 + X^4 + 12X^5 + 11X^6 + 16X^7 + 7X^8 + 2X^9 + 17X^{10} + 16X^{11} + 11X^{12} (mod\ 21)$$

Apply Offset rule with Lucas polynomial and then get Encrypted message is OCENVXSGACCQM

Encryption message of I_H

Let the Plain text be $C_1 = I_H . f_n (mod\ n)$

$$C_1 = 3 + 18X + 11X^2 + 5X^3 + 9X^4 + 16X^5 + 4X^6 + 7X^7 + 2X^8 + 16X^9 + 7X^{10} + 3X^{11} + 5X^{12} (mod\ 21)$$

Apply Offset rule with Lucas numbers and then get Encrypted message is FSPYDBLWVQTDG

Encryption message of I_I

Let the Plain text be $C_1 = I_I . f_n (mod\ n)$

$$C_1 = 6 + 5X + 8X^2 + 17X^3 + 13X^4 + 16X^5 + 11X^6 + 2X^7 + 2X^8 + 2X^9 + 3X^{10} + 12X^{11} + 20X^{12} (mod\ 21)$$

Apply Offset rule with Lucas numbers and then get Encrypted message is IFMKHBSRVCPMV

Encryption message of I_D

Let the Plain text be $C_1 = I_D . f_n (mod\ n)$

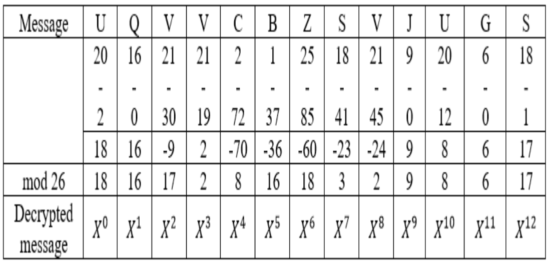
$$C_1 = 5X + 12X^2 + 14X^3 + 13X^4 + 12X^5 + 11X^6 + X^7 + 7X^8 + 2X^9 + 5X^{10} + X^{11} + 14X^{12} (mod\ 21)$$

Apply Offset rule with Lucas numbers and then get Encrypted message is CFQHHXSQACRBP

Decryption message of I_M

To get first decrypted Message take UQVVCBZSVJUGS

Now apply Reverse Offset rule with Lucas polynomials for the first decrypted message



Message	U	Q	V	V	C	B	Z	S	V	J	U	G	S
	20 - 2	16 - 0	21 - 30	21 - 19	2 - 72	1 - 37	25 - 85	18 - 41	21 - 45	9 - 0	20 - 12	6 - 0	18 - 1
	18	16	-9	2	-70	-36	-60	-23	-24	9	8	6	17
mod 26	18	16	17	2	8	16	18	3	2	9	8	6	17
Decrypted message	X^0	X^1	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	X^{10}	X^{11}	X^{12}

Fig. 4. Reverse Offset rule with Lucas polynomial

$$C_1 = 18 + 16X + 17X^2 + 2X^3 + 8X^4 + 16X^5 + 18X^6 + 3X^7 + 2X^8 + 9X^9 + 8X^{10} + 6X^{11} + 17X^{12} (mod\ 21)$$

$$I_M = f_n^{-|} C_1 (mod\ n)$$

$$I_M = (1 + X - X^2 + X^3 - X^5 + X^6 - X^8 - X^9 + X^{11} + X^{12})(18 + 16X + 17X^2 + 2X^3 + 8X^4 + 16X^5 + 18X^6 + 3X^7 + 2X^8 + 9X^9 + 8X^{10} + 6X^{11} + 17X^{12})(mod\ 21)$$

$$I_M = 5 + X + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters $5 + X + X^2 = 115 = 1001101 = M$

For the remaining characters, use the same procedure follows,

Decryption message of I_A

First decrypted Message is OCENVXSGACCQM

Reverse Offset rule with the decrypted message, get

$$C_1 = 12 + 2X + 20X^3 + X^4 + 12X^5 + 11X^6 + 16X^7 + 7X^8 + 2X^9 + 17X^{10} + 16X^{11} + 11X^{12} (mod\ 21)$$

$$I_A = f_n^{-|} C_1 (mod\ n) = 1 + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters. $1 + X^2 = 101$=1000001 $= A$

Decryption message of I_H

First decrypted Message is FSPYDBLWVQTDG

Reverse Offset rule with the decrypted message

$$C_1 = 3 + 18X + 11X^2 + 5X^3 + 9X^4 + 16X^5 + 4X^6 + 7X^7 + 2X^8 + 16X^9 + 7X^{10} + 3X^{11} + 5X^{12} (mod\ 21)$$

$$I_H = f_n^{-|} C_1 (mod\ n) = X + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters $X + X^2 = 110 = 1001000 = H$

Decryption message of I_I

First decrypted Message is IFMKHBSRVCPMV

Reverse Offset rule with the decrypted message

$$C_1 = 6 + 5X + 8X^2 + 17X^3 + 13X^4 + 16X^5 + 11X^6 + 2X^7 + 2X^8 + 2X^9 + 3X^{10} + 12X^{11} + 20X^{12} (mod\ 21)$$

$$I_I = f_n^{-|} C_1 (mod\ n) = 1 + X + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters

$1 + X + X^2 = 1001001 = I$

Decryption message of I_D

First decrypted Message is CFQHHXSQACRBP

Reverse Offset rule with the decrypted message

$$C_1 = 5X + 12X^2 + 14X^3 + 13X^4 + 12X^5 + 11X^6 + X^7 + 7X^8 + 2X^9 + 5X^{10} + X^{11} + 14X^{12} (mod\ 21)$$

$$I_D = f_n^{-|} C_1 (mod\ n) = 4 + X^2 (mod\ 21)$$

Rewrite the polynomial expression into its corresponding octal and binary representations, and then convert those binary values into ASCII characters $4 + X^2 = 104 = 1000100 = D$.

6 Conclusion and Future Work

The Lucas Polynomial Cryptosystem presents a promising addition to the cryptographic landscape, emphasizing the synergistic relationship between polynomials and Lucas numbers to create a secure and efficient encryption technique. While further exploration and analysis are necessary, the innovative properties of this cryptosystem make it a valuable contender in the quest for enhanced data security and privacy in the digital age. As the field of cryptography continues to evolve, the Lucas Polynomial Cryptosystem stands as a testament to human ingenuity in safeguarding information and protecting the fundamental principles of confidentiality and integrity.

References

[1] "Cryptograph: A very short introduction" by Fred Piper and Sean Murthy.

[2] J.Buchman"Introduction to cryptography" Springer-verlag 2001.

[3] Neal Koblitz" A course in number theory cryptography"IBSN 3-578071-8 SPIN 10893308.

[4] K.H.Rosen "Elementary number theory and its applications" Third edition,Addson Wesly.

[5] Comparison between the RSA cryptosystem and elliptic curve cryptography, Thesis by Kamilah

Abdullah .

[6] "Cryptography: A very short introduction" by Fred Piper and Sean Murthy. E.H.Lock Wood, A single-light on pascal's triangle, Math, Gazette 51(1967), PP 243-244.

[7] Fibonacci, Lucas and Pell numbers and pascal's triangle, Thomas Khoshy, Applied Probability Trust, PP 125-132.

[8] Fibonacci and Lucas Numbers with appl. Thomas Khouhy ISBN: 978-0-471-39969-8.

[9] Weisstein, Eric W. "Polynomial." *https://mathworld. wolfram. com/* (2002).

[10] Dattoli, Giuseppe, Clemente Cesarano, and Dario Sacchetti. "A note on truncated polynomials." Applied Mathematics and Computation 134.2-3 (2003): 595-605.

[11] Duran, Ugur, and Mehmet Acikgoz. "On degenerate truncated special polynomials." Mathematics 8.1 (2020): 144.

[12] Kim, T., and D. S. Kim. "Some identities on truncated polynomials associated with degenerate Bell polynomials." Russian Journal of Mathematical Physics 28 (2021): 342-355.

[13] Yang, Shuai, et al. "Context-aware text-based binary image stylization and synthesis." IEEE Transactions on Image Processing 28.2 (2018): 952-964.

[14] Alexan, Wassim, Mohamed ElBeltagy, and Amr Aboshousha. "Image encryption through lucas sequence, s-box and chaos theory." 2021 8th NAFOSTED Conference on Information and Computer Science (NICS). IEEE, 2021.

[15] Mishra, Minati, et al. "Image encryption using Fibonacci-Lucas transformation." arXiv preprint arXiv:1210.5912 (2012).

[16] Nalli, Ayse, and Pentti Haukkanen. "On generalized Fibonacci and Lucas polynomials." Chaos, Solitons & Fractals 42.5 (2009): 3179-3186.

[17] Özkan, Engin, and İpek Altun. "Generalized Lucas polynomials and relationships between the Fibonacci polynomials and Lucas polynomials." Communications in Algebra 47.10 (2019): 4020-4030.

[18] Doman, B. G. S., and J. K. Williams. "Fibonacci and Lucas polynomials." Mathematical Proceedings of the Cambridge Philosophical Society. Vol. 90. No. 3. Cambridge University Press, 1981.

[19] Gudela Ashok, S. Ashok Kumar, D. Chaya Kumari & Mathe Ramakrishna (2022) A type of public cryptosystem using polynomials and pell sequences, Journal of Discrete Mathematical Sciences and Cryptography, 25:7, 1951-1963, DOI: 10.1080/09720529.2022.2133237

[20] A. Chandra Sekhar, V. Anusha, B. Ravi Kumar & S. Ashok Kumar (2015) Linearly independent spanning sets and linear transformations for Multi-level Encryption, Journal of Information and Optimization Sciences, 36:4, 385-392, DOI: 10.1080/02522667.2014.961821.