Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1185–1194
DOI : 10.47974/JDMSC-1973

A new frontier in information security : Polynomial-Fibonacci hybrid cryptography

Gudela Ashok *
Department of Mathematics
Andhra University TDR HUB
Visakhapatnam 530003
Andhra Pradesh
India

and

Department of Mathematics
Adikavi Nannaya University
Rajamahendravaram 533296
Andhra Pradesh
India

S. Ashok Kumar †
D. Chaya Kumari §
Department of Mathematics
Gayatri Vidya Parishad College for Degree and P. G. Courses
Visakhapatnam 530045
Andhra Pradesh
India

K. V. M. Vara Kumar ‡
Department of Mathematics
Adikavi Nannaya University
Rajamahendravaram 533296
Andhra Pradesh
India

* *E-mail:* ashokavf@gmail.com (Corresponding Author)
† *E-mail:* saiashok.84@gmail.com
§ *E-mail:* chayakumari.divakarla@gmail.com
‡ *E-mail:* kalepukumar@gmail.com

Mathe Ramakrishna [@]
Department of Computer Science and Engineering
Adikavi Nannaya University
Rajamahendravaram 533296
Andhra Pradesh
India

Abstract

This research paper presents an innovative approach to fortify cryptographic systems by integrating Fibonacci polynomials into network security protocols. Leveraging the unique characteristics of polynomials and Fibonacci sequences, our methodology establishes public and private keys, enhancing message transmission security. Initial encryption with polynomials is followed by incorporating Fibonacci polynomials for an added layer of protection. Through this study, we demonstrate how Fibonacci techniques can enhance system security, providing advanced safeguards for network communications. By integrating polynomials and Fibonacci methods, our approach strengthens defense against potential threats, elevating overall system security. This innovative Polynomial-Fibonacci Hybrid Cryptography offers a promising avenue for enhancing data security in contemporary communication systems amidst escalating digital challenges.

Subject Classification: *Primary 11T71, 11B39, 11T55 Secondary 11B50, 11T06, 94A60.*

Keywords: *Cryptography, Polynomials, Fibonacci numbers, Fibonacci polynomials, Information security.*

1. Introduction

In the era of growing digitalization of the modern world, data is the new currency which over took all the conventional norms. The many aspects of daily life that have been digitalized ranges right from personal information to online transactions, though this recent advancement made the lives of human easy there also comes the potential external side effects in the form of cybercrimes and data threats. To counter-act this, the encryption and decryption tools acts as the weapons, where the sensible data is initially encrypted and then decrypted between the sender and receiver to provide optimal level of chain of security. This study focuses on using the field of cryptography with the polynomials and Fibonacci numbers [1][2][3].

Cryptography plays a crucial role in augmenting the security of message transmission in a secure manner [4]. To further enhancing the

[@] *E-mail:* `mathe.ramakrishna@gmail.com`

security. We exploit the properties of polynomials are to be uncalculated in public key cryptography. We annihilate the properties of Fibonacci [5] using codes by constructing a public key cryptosystem is established.

2. Definitions and Standard results

General form of polynomials is $P(x) = P_0(x) + \alpha P_1(x) + \ldots + \alpha^n P_n(x)$.

2.1 *Modular Arithmetic*

Modular arithmetic involves integer calculations where numbers cycle back after reaching a modulus value. It's crucial in number theory, algebra, and cryptography, like RSA. Operations include addition, subtraction, multiplication, division, exponentiation, and finding inverses. Validity depends on modulus properties, like primality or relative primality [6].

Example: Take $= x + x^2$ and $b = 2x + 5x^3 \Rightarrow ab = 5x^5 + 5x^4 + 2x^3 + 2x^2$, each coefficient by its remainder by 2 then $ab(\text{mod}\,2) = x^5 + x^4$.

2.2 *Truncated Polynomial:*

A truncated polynomial is a polynomial in which terms of order N or higher are removed. This means that the polynomial is reduced to a specific degree and the coefficients are only allowed to take values in a certain range. The polynomial operations can be performed quickly using the Number Theoretic Transform. By reducing the polynomials modulo X^N-1, which is imp for the security of the system.

For example $N = 3$, $a = x + x^2$ and $b = 1 + x$ Thus, $ab = x + 2x^2 + x^3 \notin T$

For the following rule, $ab = x + 2x^2 + x^0 = 1 + x + 2x^2 \in T$ [6].

2.3 *Cryptography:*

It is a Science of using Mathematics to send information behind encryption. It involves storing private data with a key. The strength of cryptography depends on the resources and time complexity. Algorithms constructed through Cryptography are more complex and unique.

2.4 *Types of Cryptography:*

2.4.1 Symmetric cryptography

It uses identical key for both encryption and decryption.[7][8]

2.4.2 Asymmetric cryptography

It uses distinct keys for both encryption and decryption.[7][8]

2.5 Fibonacci sequence

Fibonacci sequences find widespread application in numerous computer algorithms and cryptographic techniques. These numbers are defined by the recurrence relation $F_{n+1} = F_n + F_{n-1}$, with initial conditions $F_1 = F_2 = 1$ [7][8].

2.6 *Fibonacci polynomial*

The Fibonacci polynomial are defined by the recurrence relation $F_{n+1}(x) = xF_n(x) + F_{n-1}(x)$, With $F_1(x) = 1$ and $F_2(x) = x$, $F_3(x) = x^2 + 1$, $F_4(x) = x^3 + 2x$, $F_5(x) = x^4 + 3x^2 + 1$ [4][5][7][8].

3. Algorithm

3.1 *Encryption method*

- Choose two large integer *p, q* such that *(p, q) =1* and choose a random polynomial *f*
- Determine $n = pq$ and Compute $f_n(\mathrm{mod}\, n)$ [9]
- Please express the ASCII numerical equivalent of the plain text message '*m*' as 'm_1'
- Convert the ASCII numerical equivalent m_1 to binary and make it publicly available.
- Produce the polynomial representing the initial encryption level of message m_1.
- Calculate the Cipher text $C_1 = m_1 f_n(\mathrm{mod}\, n)$
- Utilize the offset rule of Fibonacci numbers or Fibonacci polynomials on the ciphertext $C_1$to generate a super-encrypted text C_2 & transmit it to the intended recipient [10][11][12][13].

3.2 *Decryption method*

- Upon receiving the super-encrypted text C_2 from the sender, decrypt it using the secret method, which involves reversing the offset rule of Fibonacci numbers or Fibonacci polynomials. Denote the decrypted result as m_1'.
- The recipient further decrypts the text m_1' using the equation $m_2' \equiv f_n^{-1} m_1' (\mathrm{mod}\, n)$.
- Transform m_2' into its corresponding binary representation.
- Translate the obtained binary values into ASCII characters to retrieve the plaintext message *m* [14][15].

4. Demonstration with Fibonacci numbers:

Step 1: Let us choose two integers $p = 2$ and $q = 11$ and take polynomial f,

$$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10} + x^{11} + x^{12}$$

Step 2: Compute $n = 2 \times 11 = 22$ and find $f_n (\mathrm{mod}\, n)$

$$f_n = 11x + 12x^2 + 19x^3 + 5x^4 + x^5 + 5x^6 + 19x^7 + 4x^8 + 10x^{10} + 5x^{11} + 12x^{12} (\mathrm{mod}\ 22)$$

And also find $f_n^{-1} (\mathrm{mod}\, n)$

$$f_n^{-1} = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10} + x^{11} + x^{12} (\mathrm{mod} 22)$$

Step 3: Let's consider the plain text message "ASHOK". Determine its ASCII numerical equivalent [16][17], then convert it to binary. Subsequently, formulate its polynomial representing as the first level of encryption in the following manner:

$A = 1000001, S = 1010011, H = 1001000, O = 1001111$ and $K = 1001011$

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

$$\boldsymbol{A} = 1 + x^6, \boldsymbol{S} = 1 + x + x^4 + x^6, \boldsymbol{H} = x^3 + x^6,$$
$$\boldsymbol{O} = 1 + x + x^2 + x^3 + x^6, \boldsymbol{K} = 1 + x + x^3 + x^6$$

Let us take the pain text ASHOK into polynomials $\boldsymbol{I}_A, \boldsymbol{I}_S, \boldsymbol{I}_H, \boldsymbol{I}_O$ and $\boldsymbol{I}_K$ respectively.

Encryption message of $\boldsymbol{I_A}$ *:*

Step 4: Calculate the second level of encryption using I_A, find $C_1 = I_A f_n(\text{mod}\, n)$.

$$C_1 = 19 + 15x + 12x^2 + 7x^3 + 10x^4 + 13x^5 + 5x^6 + 8x^7 + 16x^8 + 19x^9 + 15x^{10} + 6x^{11} + 17x^{12} (\text{mod}\, 22)$$

Step 5: Utilize the offset rule with Fibonacci numbers to encrypt C_1 and obtain the super-encrypted text C_2 [17].

Table 1

Encryption of $\boldsymbol{I_A}$

	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}
	19 + 1	15 + 1	12 + 2	7 + 3	10 + 5	13 + 8	5 + 13	8 + 21	16 + 34	19 + 55	15 + 89	6 + 144	17 + 233
	20	16	14	10	15	21	18	29	50	74	104	150	250
mod 26	20	16	14	10	15	21	18	3	24	22	0	20	16
Encrypted message	U	Q	O	K	P	V	S	D	Y	W	A	U	Q

Super encrypted message is UQOKPVSDYWAUQ

For the remaining characters, we use the same procedure follows,

Encrypted text of I_S*:*

Consider the Plain text is $C_1 = I_S f_n(\text{mod}\, n)$ and Fibonacci numbers used for offset rule yield "KEIMMPFFAFFBD" as the super encrypted message.

Top of Form

Encrypted text of I_H*:*

Consider the Plain text is $C_1 = I_H f_n(\text{mod}\, n)$ and Fibonacci numbers used for offset rule yield "IKONVKGLVFNTE "as the super encrypted message (as shown in Table 1).

Encrypted text of I_O*:*

Consider the Plain text is $C_1 = I_O f_n(\text{mod}\, n)$ and Fibonacci numbers used for offset rule yield "DLPLNNVOBGBIJ"as the super encrypted message.

Encrypted text of I_K:

Consider the Plain text is $C_1 = I_K f_n (\mathrm{mod}\, n)$ and Fibonacci numbers used for offset rule yield "UVPWXQQNWJXI"as the super encrypted message (as shown in Table 2).

Decrypted text of I_A:

Step 1: Take into account the super-encrypted message of I_A as UQOKPVSDYWAUQ.

Step 2: Employ the reverse offset rule of Fibonacci numbers (Secret key) [7][11][12][13].

Table 2

Decryption of I_A

Message	U	Q	O	K	P	V	S	D	Y	W	A	U	Q
	20	16	14	10	15	21	18	3	24	22	0	20	16
	20	16	14	10	15	21	18	3	24	22	0	20	16
	-	-	-	-	-	-	-	-	-	-	-	-	-
	1	1	2	3	5	8	13	21	34	55	89	144	233
	19	15	12	7	10	13	5	-18	-10	-33	- 89	-124	-217
mod 26	19	15	12	7	10	13	5	8	16	19	15	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}

$$C_1 = 19 + 15x + 12x^2 + 7x^3 + 10x^4 + 13x^5 + 5x^6 + 8x^7 + 16x^8 + 19x^9 + 15x^{10} + 6x^{11} + 17x^{12} (\mathrm{mod}\, 22)$$

Step 3: Compute $I_A = f_n^{-1} C_1 (\mathrm{mod}\, n)$

$$I_A = 23 + 44x + 44x^2 + 244x^3 + 22x^4 + 22x^5 + 45x^6 + 44x^7 + 44x^8 + 22x^9 + 44x^{10} + 66x^{11} + 22x^{12} (\mathrm{mod}\, 22)$$

$$I_A = 1 + x^6 (\mathrm{mod}\, 22)$$

The polynomial $1 + x^6$ is converted into its respective binary representation 1000001, which is then converted into the ASCII character '*A*'.

For the remaining characters, we use the same procedure follows,

Decrypted text of I_S:

The Super encrypted message I_S decodes to KEIMMPFFAFFBD using reverse offset $I_S = f_n^{\dashv} C_1 \pmod{n} = 1 + x + x^4 + x^6 \pmod{22} \Rightarrow 1010011 = S$

Decrypted text of I_H**:**

The Super encrypted message I_H decodes to IKONVKGLVFNTE using reverse offset $I_H = f_n^{\dashv} C_1 \pmod{n} = x^3 + x^6 \pmod{22} \Rightarrow 1001000 = H$

Decrypted text of I_O**:**

The Super encrypted message I_O decodes to DLPLNNVOBGBIJ using reverse offset $I_O = f_n^{\dashv} C_1 \pmod{n} = 1 + x + x^2 + x^3 + x^6 \pmod{22} \Rightarrow 1001111 = O$

Decrypted text of I_K**:**

The Super encrypted message I_K is decodes to UVPWXQQNWJXI using reverse offset $I_K = f_n^{\dashv} C_1 \pmod{n} = 1 + x + x^3 + x^6 \pmod{22} \Rightarrow 1001011 = K$

5. Enhancing Security with Fibonacci Polynomials

Similarly, we can apply the same process using Fibonacci polynomials instead of Fibonacci numbers. Using Fibonacci polynomials, the security of keys is significantly strengthened, making them harder to crack, resulting in increased computational time.

6. Discussion and Conclusion

Public key cryptosystems like RSA are often considered more secure than symmetric key cryptosystems for specific applications, although this isn't universally true. Security depends on various factors including key strength and encryption algorithm quality. Symmetric key systems may outperform public key systems in some cases. Time complexity is crucial; public key systems typically have higher complexity, impacting practical performance. However, the efficiency of a cryptographic algorithm depends on implementation and hardware. Thus, symmetric key systems can be more efficient than public key systems in certain scenarios.

References

[1] Piper, Fred, and Sean Murthy. Cryptograph: A Very Short Introduction.

[2] Buchman, J. Introduction to Cryptography. Springer-Verlag (2001).

[3] Koblitz, Neal. A Course in Number Theory and Cryptography. IBSN 3-578071-8 SPIN 10893308.

[4] Ranasinghe, Rajitha, Chathurangi, Madusha & Athukorala, Pabasara. A novel improvement in RSA algorithm, *Journal of Discrete Mathematical Sciences and Cryptography*, 27:1, 143–150 (2024), DOI: 10.47974/JDMSC-1628.

[5] Philippou, A. N., et al., editors. Application of Fibonacci Numbers. Springer Science Media LLC.

[6] Clark, Benjamin, "Understanding the NTRU Cryptosystem" *Williams Honors College, Honors Research Projects*. 906 (2019).

[7] Mukhopadhyay, S. K., et al. "An ECG Signal Compression Technique Using ASCII Character Encoding." Measurement, vol. 45, no.6, pp. 1651-1660 (2012).

[8] Panwar, Yashwant K., et al. "Generalized Fibonacci Polynomials." *Turkish Journal of Analysis & Number Theory*, vol. 1, no. 1, pp. 43-47 (2013).

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

[10] Piper, Fred, and Sean Murphy. Cryptography: A very short introduction. Vol. 68. Oxford Paperbacks (2002).

[11] Sekhar, A. Chandra, S Ashok Kumar. "Symmetric Key Cryptosystem for Multiple Encryptions." *International Journal of Mathematics Trends and Technology* (IJMTT), vol. 29 (2016).

[12] Sekhar, A. Chandra, S Ashok Kumar. "Triple Encryption Scheme Using Two Independent Keys."

[13] Rao, K. Subba. "Some Properties of Fibonacci Numbers." The American Mathematical Monthly, vol. 60, no. 10, pp. 680-684 (1953), doi: 10.1080/00029890.1953.11988390.

[14] Bisht, Nivedita, and Sapna Singh. "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms." *International Journal of Innovative Research in Science, Engineering and Technology,* vol. 4, no. 3, pp. 1028-1031 (2015).

[15] Kumar, Ankit, et al. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 491-498 (2019).

[16] Khoshy, Thomas. Fibonacci and Lucas Numbers with Applications. ISBN: 978-0-471-39969-8.

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