ANALYSIS OF FIBONACCI SERIES & CRYPTOGRAPHY

Akansha Agarwal¹, Dr. B.K Singh²

¹Research Scholar, IFTM University, Moradabad (U.P), India.
²Professor, IFTM University, Moradabad (U.P), India.

Abstract: This paper will explain the properties of Fibonacci numbers that can be stated and proved for a much more universal class of sequence namely, second order recurrences. Fibonacci numbers in different forms are widely applied in constructing security coding. This paper will also analyze a cryptography method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration but also it can be used for user authentication.

Keywords: Cryptography, Security, Encryption, Decryption, Integrity, Authentication.

1. INTRODUCTION:

The objective of cryptography is to make it feasible for two persons to exchange a message in such a way that other persons cannot understand. There is no end to the number of ways this can be done, but here the proposed method will be more concerned with a technique of encoding the text in such a way that the recipient can only discover the original message. The original message usually called plain text is converted into cipher text by finding each character in the message and replacing it with another character based on the Fibonacci number generated. Further cipher text is converted into Unicode symbols, which avoid suspicion from the third party when send through an unsecured communication channel.

There are two steps in the proposed method:

- Conversion from plain text to cipher text.
- Convert cipher text to Unicode symbols.

In both level, security key is used to encode the original message which provides two levels of security from intruders. On the other end, the extraction algorithm is designed in such a way that the process converts the Unicode symbols into cipher text and then cipher text to plain text. This encoding and decoding scheme of the proposed method is radically different as compared to the conventional methods.

2. FIBONACCI NUMBERS:

Fibonacci is one of the most famous names in mathematics. This would come as a surprise to Leonardo Pisano, the mathematician we now know by that name. he might have been equally surprised that he has been immortalized in the famous sequence – 0, 1, 1, 2, 3, 5, 8, 13, ... – rather than for what is considered his far greater mathematical achievement – helping to popularize our modern number system in the Latin-speaking world.

Fibonacci Primes:

A Fibonacci prime, as you should easily guess is a Fibonacci number that is prime. Recall that the Fibonacci numbers can be defined as follows:

\[ F_1 = F_2 = 1, \]
\[ F_{n+1} = F_n + F_{n-1}, \]
where \( n > 2 \)

It is easy to show that \( F_n \) divides \( F_{n+1} \), so for \( F_n \) to be a prime, the subscript must either be 4 (because \( F_2 = 1 \)) or a prime. This however is not sufficient!

Golden Ratio:

If we take the ratio of two successive numbers in Fibonacci series, dividing each by the number before it, we will find the following series of numbers: 1/1 = 1, 2/1 = 2, 3/2 = 1.5, 5/3 = 1.666..., 8/5 = 1.6, 13/8 = 1.625, 21/13 = 1.61538 ………

A graph of these values you'll see that they seem to be tending to a limit, which we call the golden ratio it is also known as the golden number and golden section.

Figure 1: Graph for Fibonacci Numbers
1/1, 2/1, 3/2, 5/3, 8/5 ………Ratio of successive Fibonacci terms.

It has a value of \((\sqrt{5} + 1)/2\) (approximately 1.618034) and is often represented by a Greek letter Phi, written as \(\Phi\). The closely related value which we write as \(\phi\), a lowercase phi, is just the decimal part of Phi, namely 0.618034... \((\sqrt{5} - 1)/2\), the number that accounts for the spirals in the seed heads and the arrangements of leaves in many plants. But why do we see phi in so many plants? The number Phi (1.618034...), and therefore also phi (0.618034...), are irrational numbers: they can't be written as a simple fraction. Let's see what would happen if the meristem in a seed head instead turned by some simpler number, for example the fraction 1/2. After two turns through half of a circle we would be back to where the first seed was produced. Over time, turning by half a turn between seeds would produce a seed head with two arms radiating from a central point, leaving lots of wasted space.

3. CRYPTOGRAPHY:

With the technology advancements and easy availability of internet, every day millions of users share information electronically through emails, file sharing, e-commerce, etc. As, internet is highly vulnerable to various attacks, sending sensitive information over the Internet may be dangerous. One of the ways to protect the sensitive Information is using the cryptographic techniques. So, while sharing sensitive information over the Internet, it should be sent in encrypted form to prevent the access by unauthorized person. Encryption can be defined as the process of transforming information in such a manner that only authorized person can understand the shared information.

Modern cryptography concerns:

- **Confidentiality**: Information cannot be understood by anyone else except for the person intended to.
- **Integrity**: Information cannot be altered.
- **Non-repudiation**: Sender cannot deny his/her intention in the transmission of the information at a later stage.
- **Authentication**: sender and receiver can confirm each other.

Cryptography is used in many applications like banking transactions, cards, computer passwords, and e-commerce transactions.

Three types of cryptographic techniques used in general.

Symmetric Key Cryptography:

Both the sender and receiver share a single key. The sender uses this key to encrypt plain text and send the cipher text to the receiver, on the other side the receiver applies the same key to decrypt the message and recover the plain text.

Public Key Cryptography:

This is the most revolutionary concept in the last 300-400 years. In the public-key cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key remains a secret. The public key is used for encryption and for decryption private key is used.

Hash functions:

No key is used in this algorithm. A fixed length has value computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash function are also used by many operating systems to encrypt passwords.

4. ENCRYPTION/ DECRYPTION BY USING FIBONACCI SEQUENCE:

The Fibonacci sequence is a linear recurrence of the form \(F_n = F_{n-1} + F_{n-2}\). so each term is made by adding the preceding two terms of the sequence. Changing the meaning to some extent can lead to an entire family of recurrences based on the Fibonacci sequence. A value \(p\) can be used in the sequence to give an changed by the formula: \(F_p(i) = F_p(i - 1) + F_p(i - p - 1)\). For the Fibonacci sequence, this p-value is 1, then resulting in the sequence will be 1,2,3,5,8,13,... or sometimes 1,1,2,3,5,8,13,... . To add variation to the sequence, the value of \(p\) can simply be changed so that the sequence will follow a different pattern. For encryption purposes, choosing a \(p\)-value other than 1 may decrease the likelihood that the sequence will be known, thus heightening the security of the encryption. In order to begin the encryption of a number, it is crucial to know the initial \(p\) (prime)-value. Each number ‘n’ is encoded as a codeword consisting of the sequence indices of the sequence terms that add to achieve ‘n’. The process begins with choosing the largest term less than or equal to ‘n’ and proceeds by subtracting that largest term from ‘n’. Putting together the values that sum to ‘n’ in this manner is a concept known as the greedy algorithm. The indices of 9 the terms are then used to encode that number.

For example: using \(p = 3\) (with the indices beginning at 0 rather than 1, which is the sequence used in Goriely & Moulton, 2012).

Fibonacci sequence:

0,1,2,3,4,5,7,10,14,19,26,36,50,59,85,121,...

If \(n = 35\) can be written as 26 +7 +2 then the encoded form will be 020610

If \(n = 90\) can be written as 85 + 5 then the encoded form will be 0615.
If \( n = 100 \) can be written as \( 85 + 14 + 1 \) then the encoded form will be \( 010814 \).

In the above examples, the integer 35 is found by first subtracting the largest number from the sequence that is less than or equal to 35. Now the number 26 is less than 35 is subtracted and this difference is equal to 9. Now number 7 is less than 9 is subtracted again and this difference is 2. The index of 2 is 02, the index of 7 is 06 and the index of 26 is 10. Thus, the encoded form of 35 is 020610. The remaining numbers \( n = 90 \) and \( n = 100 \) are encoded in the similar approach. To decode a set of numbers, the same concept applies in reverse. The main necessity for the decoding party is the initial p-value so the decoder knows what sequence he/she is working with. After acquiring that, the sequence can be found from the equation, then the encoded numbers are simply the term numbers. Those terms can be added up to equal the final value, which stands for a specific page, line, or character number. This method of encryption and decryption is adapted from the method used in Sherlock Holmes (Goriely & Moulton, 2012).

REFERENCES: