Punjab University Journal of Mathematics (2024), 56(6), 230-250
https://doi.org/10.52280/pujm.2024.56(6)01

Applications of Fourier Transformation with the help of Cryptography

Muhammad Haroon Aftab, Shakeela Rehman.
Department of Mathematics,
The University of Lahore, Lahore, 54000, Pakistan,
Email: haroonuet@gamil.com, komalchanda81@gmail.com

Received: 19 April, 2023 / Accepted: 01 January, 2025 / Published online: 31 January, 2025

Abstract. Cryptography is used for the investigation of mathematical skills that interlink with the aspects of data integrity, individual authentication, and information security. Cryptography is the fundamental basis of modern electronic communication. The Encryption means converting a file into secret keys, while decryption means converting an encrypted message into normal language. Numeric values from 0 to 25 and 26 to 51 will be assigned to small and capital alphabets, respectively. The special case of Taylor series will be considered for exponential and simple functions. Fourier transformation will be used to code and decode a message. For better calculation of encryption and decryption, the modulus 57 will be used with 4 special characters. Many researchers have utilized different transformations such as Laplace and natural transformations. However, Fourier transformation with exponential function has provided authentic results compared to other transformations. The key factor of this work is the generalized key that decodes the special information, including ATM cards transmitting financial information and computer passwords. Cryptography is the study of mathematical skills related to information security aspects such as confidentiality, data integrity, data authentication, and personal authorship. Fourier Transforms, a powerful mathematical tool used to analyze and manipulate signals in the frequency domain, have found numerous applications in the field of cryptography. By transforming data between the time and frequency domains, Fourier methods offer unique advantages for encryption, decryption, and the design of cryptographic algorithms

AMS (MOS) Subject Classification Codes: 11T71; 68P25; 15A04; 11F30
Key Words: Cryptography, encryption, transformation, Laplace, Mellin, Fourier, decryption..

1. Introduction

Privacy is a top priority for everyone. Personal document integrity is the most challenging thing during this period. To address this challenge, we're on our way to the world of crypto. Encryption [1] provides us with the opportunity to share information with others, with the involvement of a third party without any risk to your privacy. Cryptography uses the method of encryption for sending information from one place to another or storing data. The decryption method is for decoding data.

Presently, because of cybercrime, privacy is the most important reality. Anybody needs to protect data, documents, secret messages, and personal networks. The most popular gadget among us is the cell phone. Because of the privacy issue, several websites are locked. For this reason, just because of the word cryptography can be anything. Cryptography is an incredibly vast subject for research Anshel [2] and Blakley [3]. It is the mixture of the purposes of mathematics, electrical engineering, computer science, and subverting designers. Follow the crowd, as some analysis did a few weeks, you can use power crypt analyticity in the world Schneider [22].

Cryptography is the study of mathematical skills related to information security [5, 10] aspects such as confidentiality, data integrity, data authentication, and person authorship. Cryptography's aim is that the person who is qualified can only read the given data; nobody else can read the data. The assurance is given to the receiver that the data do not shift. Message authentication also says receiver authentication of the data origin is achieved by some sources Buchman [4]. If somebody wants to hide a confidential message in some way, then the sender used that method is called the cipher [21] text method. Cryptography has been used to encrypt passwords, smart cards in banking applications, stable websites, and code breaks during World War II. An encryption machine called the German Enigma was used in World War II. Typically, cryptography applies to modern electronic communications. The system used in ancient Greece for writing is called the scytale. Actually, cryptography is the study of code writing with the purpose of hiding the meaning of any secret message. Security is the basic requirement of every human being in day-to-day life in various tasks. Information in the modern world deals with electronic devices and the internet in a multimedia form. The safe and secure storage and communication of data over the internet is essential. Most of the data is transmitted in the form of images, so image encryption algorithms come into view. These algorithms convert the image to be stored or transmitted into an intelligible form so that unauthorized users will not be able to gain any knowledge from them. The conversion of the original image into the unreadable image is known as an encrypted image by implementing an algorithm, and a special set of characters is known as the key to the input image.

The decryption process is normally the reverse of the encryption process. There are a number of digital and optical encryption techniques and cryptosystems developed in the past decades for protected and unharmed data storage and transmission. Digital techniques use various cryptographic algorithms based on stream and block cipher concepts. In the optical field of encryption, the classical approach used relies on Double Random Phase Encoding (DRPE) system in which two random phase masks are deployed as the keys for both the encryption and decryption process. One of them is applied in the input plane and the second one in the Fourier plane proposed by Refrgier et. al. [19].

In the field of optical information processing, the optical encryption techniques play a crucial role in providing reliable data security. This letter focuses on the use of Fourier transforms for image encryption. Fourier Transform is derived from the concept of Fourier series and is used to convert signals from the time or spatial domain to the frequency domain. According to Fourier transformation, any signal can be represented as a combination of sine and cosine signals. Fourier transformation is an important image processing tool that breaks down an image into its sine and cosine components and outputs transformed images in the frequency domain. It also introduces an additional parameter of security, namely the fractional order in the encryption scheme. The remainder of the paper consists of literature demonstrating the use of Fourier transformation in the context of image encryption. Many techniques and approaches that have been developed in the last two decades are surveyed in this paper. Their related pros and cons are discussed. The security provided by the proposed work is examined in this paper and the comparison of some approaches differing in the key space for the encryption algorithm is also presented here. The results show the techniques that are more resistant to attacks and hence offer more security.

2. Preliminaries

2.1. **Cryptography.** Privacy is a top priority for everyone. Personal document integrity is the most challenging thing during this period. To address this challenge, we're on our way to the world of crypto. Encryption provides us with the opportunity to share information with others, with the involvement of a third party, without any risk to your privacy. Cryptography uses the method of encryption for sending information from one place to another or storing data. The decryption method is used for decoding data.

2.2. **Terminology in cryptography.**

2.2.1. *Cryptography.* Cryptography is associated with the study of mathematical techniques to provide information about security services.

2.2.2. *Cryptanalysis.* Cryptanalysis is associated with learning mathematical techniques to crack security services.

2.2.3. *Cryptology.* Cryptology is associated with the study of cryptography and cryptanalysis.

2.2.4. *The Plain text.* Clear text, also known as plaintext, is written in simple English so that it can be easily understood by everyone it. It can consist of a single word or sentence.

2.2.5. *The Cipher text.* The ciphertext is the text obtained after applying appropriate algorithms or methods to the plaintext. The ciphertext is impossible to read and understand except by the one who has the key to decrypt the data.

2.2.6. *Cipher types.* There are different types of ciphers here that we will discuss, some of them

(1) Cease cipher
(2) Monoalphabetic cipher
(3) Homophonic substitution cipher
(4) Hill cipher

(5) Encryption
(6) Decryption
(7) Porta cipher
(8) Autokey cipher
(9) Cipher input PolyGram
(10) Playfair cipher
(11) Transposition cipher

2.3. **Applications.** Fourier transformation, a mathematical technique that decomposes a signal into its constituent frequencies, has found surprising applications in the field of cryptography. While not as direct as some other cryptographic tools, Fourier transformation's ability to analyze and manipulate signals in the frequency domain offers unique advantages in certain cryptographic contexts.

2.3.1. *Linear Cryptanalysis.* The Fourier transform can be used to analyze the correlation between linear combinations of plaintext bits and ciphertext bits, helping to break certain block ciphers.

2.3.2. *Differential Cryptanalysis.* By analyzing the differences in ciphertext distributions after specific input differences, the Fourier transform can aid in identifying weaknesses in block ciphers.

2.3.3. *Side-Channel Attacks.* The Fourier transform can be used to analyze power consumption or electromagnetic emanations from cryptographic devices, potentially revealing secret keys.

2.3.4. *Steganography.*

2.3.5. *Hiding Data in Signals.* Fourier transform can be used to embed secret messages within seemingly innocuous signals, such as images or audio files, by manipulating specific frequency components.

2.3.6. *Detecting Steganography.* By analyzing the frequency spectrum of a signal, Fourier transform can help detect hidden messages, although sophisticated steganographic techniques can make this challenging.

2.3.7. *Homomorphic Encryption.*

2.3.8. *Secure Signal Processing.* Fourier transform can be performed on encrypted data using homomorphic encryption schemes, enabling secure signal processing tasks without revealing the underlying data.

2.3.9. *Privacy-Preserving Machine Learning.* Fourier transform can be used in privacy-preserving machine learning algorithms, allowing models to be trained and evaluated without exposing sensitive data.

2.3.10. *Research and Development.*

2.3.11. *New Cryptographic Primitives.* Researchers are exploring the use of the Fourier transform to design new cryptographic primitives, such as digital signatures and encryption schemes, with improved security and efficiency.

2.3.12. *Post-Quantum Cryptography.* Fourier transform-based techniques are being investigated for their potential resistance to quantum computer attacks, which could break many existing cryptographic algorithms.

2.4. **Challenges and Limitations.**

2.4.1. *Computational Complexity.* Performing the Fourier transform on large datasets can be computationally expensive, especially for high-dimensional data.

2.4.2. *Sensitivity to Noise.* The Fourier transform can be sensitive to noise in the input signal, which can degrade the accuracy of cryptographic analysis or steganography.

2.4.3. *Security Concerns.* While the Fourier transform can be used for both offensive and defensive purposes in cryptography, it is important to consider the potential security implications of its use.

2.5. **Conclusion.** The Fourier transformation is a versatile tool with a growing number of applications in cryptography. Its ability to analyze and manipulate signals in the frequency domain offers unique advantages in cryptanalysis, steganography, homomorphic encryption, and other areas. As research in this field continues, we can expect to see even more innovative and powerful cryptographic techniques based on the Fourier transform.

3. MATERIAL AND METHODS

Cryptography's main aim is to protect our system using several techniques, including methods for transformation. Cryptography involves two types of text: plaintext and ciphertext.

Humans read simple messages called plaintext, and while coded messages that are readable only by the receiver are called ciphertext. The encryption of a secret message is done from plaintext to ciphertext and the reverse process is called decryption. For this purpose, the Laplace and Sumudu transformations are used.

The Sumudu transform is a type of ordinary differential equation with both integer and non-integer order derivatives. In this case, we will apply the double Sumudu transform to solve a non-homogeneous wave equation with a convolution term, where the non-homogeneous term is a double convolution. We can directly apply it to fractional type ordinary differential equations, both homogeneous and non-homogeneous ones.

To apply the Fourier transformation to ensure our system is stable, any change is used to protect personal information must have its opposite.

3.1. **Use of transformations.** In cryptography, two transformations were applied: one is the Laplace transformation, and the Sumudu transformation is another Debnath transformation written by Debnath, with the assistance of Taylor Series.

3.2. **Laplace transformation.** The Laplace transformation can be defined as Papoulis [16].

$$L\{z(v)\} = F(u) = \int_0^\infty e^{-uv} z(v)\, dv,$$

and the inverse of Laplace Transformation exists, which can also be defined as

$$L^{-1}\{z(v)\} = \frac{1}{2\lambda i} lim_{x \longrightarrow \infty} \int_{y-ix}^{y+ix} e^{uv} z(u)\, du.$$

3.3. **Mellin transformation.** It is an integral transformation which was named by the mathematician Hjalmar Mellin. It is defined as

$$M[g(x); h] = \int_0^\infty g(x) x^{h-1}\, dx.$$

Hjalmar Mellin also defined the inverse Mellin transformation as

$$M^{-1}[g(x); h] = \frac{1}{2\lambda i} \int_{c+i\infty}^{c-i\infty} g(x) x^{(-h)}\, dx.$$

Which is the line integral in the complex plane. Mellin transformation is very useful for the study of zeta functions, which are used in number theory to check the properties of prime numbers. Mellin transformation also play a necessary role in mathematical statistics, number theory, and the theory of Dirichlet series and many other subjects.

3.4. **Some theorems and standard results.** Some standard theorems are used for coding and decoding personal information and explaining their results.

Proposition 1

The given plaintext is in terms of Sa, 0, where a = 1, 2, 3, 4, ... , under the Mellin transformation of any suitable function. Then this function is multiplied by any coefficient to obtain the ciphertext.

$$S_{(a,1)} = 2^{(2a+1)}(2a+2)(2a+3)S_{(a,0)}\ mod\, 257,$$
$$S_{(a,1)} = Q_{(a,1)} - 26K_{(a,1)},\ for\ a = 0, 1, 2, 3, ...$$
$$Where,\ Q_{(a,1)} = 2^(2a+1)(2a+2)(2a+3)S_{(a,0)}\ for\ a = 0, 1, 2, 3, ...$$
$$And\ K_{(a,1)} = \frac{Q_{(a,1)} - S_{(a,1)}}{57}\ for\ a = 0, 1, 2, 3, ...$$

Here, Q denotes the quotient, S for denoting the plaintext, and K denotes the key.

Proposition 2

Given plaintext is in terms of Sa,1, where a = 1, 2, 3, 4, . . . under Mellin transformation of any suitable function by Sa,0 then this function is multiplied by any coefficient for getting the cipher text.

$$S_{(a,2)} = S_{(a,1)} 2^{(2a+1)}(2a+2)(2a+3)\ mod\ 257.$$

Proposition 3

Given plaintext is in terms of Sa, 0, where a = 1, 2, 3, 4, . . . under Mellin transformation of any suitable function successively j times, then this function is multiplied by any coefficient for getting cipher text.

$$S_{(a,j)} = S_{(a,j-1)}2^{(2a+1)}(2a+2)(2a+3)\ mod\ 257,$$
$$S_{(a,j)} = Q_{(a,j-1)} - 26K_{(a,j)}\ for\ a = 0,1,2,3,....$$
$$Where,\ Q_{(a,j)} = S_{(a,j-1)}2^{(2a+1)}(2a+2)(2a+3)\ for\ a = 0,1,2,3,....$$
$$And\ key\ is\ K_{(a,1)} = \frac{Q_{(a,j)} - S_{(a,j)}}{57}\ for\ a = 0,1,2,3,....$$

Here Q denotes the quotient, S for denoting plaintext and K denotes key. When j = 1 then first theorem applies and when j = 2 then second theorem apply.

Proposition 4

Generalization of these results is obtained by taking a more general function except this procedure remains the same for getting the ciphertext $S_{(a,1)}$ from plaintext $S_{(a,0)}$.

$$WhereQ_{(a,h)} = S_{(a,0)}g^{(2a+1)}(2a+2)(2a+3)...(2a+h+1)\ a,h = 0,1,2,3....$$

And the key for the general function is defined as

$$K_{(a,h)} = \frac{Q_{(a,h)} - S_{(a,h)}}{57}\ for\ a = 0,1,2,3,....$$

Theorem 1

If f(x) is an even function, then

(1)

$$\overline{f(w)} = 2\int_0^\infty f(x)cos(wx)\,dx.$$

(2)

$$f(x) = \frac{1}{\pi}\int_0^\infty \overline{f(w)}cos(wx)\,dw.$$

Proof 1

By definition we know that

$$\overline{f(w)} = \int_{-\infty}^{\infty} e^{-iwx}f(x)\,dx = \int_{-\infty}^{\infty} (\cos(wx) - i\sin(wx))\,f(x)\,dx$$
$$= \int_{-\infty}^{\infty} f(x)\cos(wx)\,dx - i\int_{-\infty}^{\infty} f(x)\sin(wx)\,dx \quad \text{Equation (a).}$$

The second integral in equation (a) is zero because the function f(x) is an even function, therefore f(x) cos(wx) is even and f(x) sin(wx) is odd. So, the equation (a) becomes

$$\overline{f(w)} = 2\int_0^\infty f(x)cos(wx)\,dx.$$

Proof 2

By definition, we know that

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx}\,\overline{f(w)}\,dw = \frac{1}{2\pi}\int_{-\infty}^{\infty} (\cos(wx) + i\sin(wx))\,\overline{f(w)}\,dw$$
$$= \frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\cos(wx)\,dw + i\frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\sin(wx)\,dw \quad \text{Equation (b).}$$

By part (1)

$$\overline{f(-w)} = 2\int_{0}^{\infty} f(x)\cos(-wx)\,dx,$$
$$\overline{f(w)} = 2\int_{0}^{\infty} f(x)\cos(wx)\,dx.$$

The second integral on R.H.S of equation (b) is zero because the function in second integral $\overline{f(w)} sin(wx)$is an odd function. So, we have

$$f(x) = \frac{2}{2\pi}\int_{0}^{\infty} \overline{f(w)}\cos(wx)\,dw,$$
$$f(x) = \frac{1}{\pi}\int_{0}^{\infty} \overline{f(w)}\cos(wx)\,dw.$$

Theorem 2
If f(x) is an odd function, then

(1)
$$\overline{f(w)} = -2i\int_{0}^{\infty} f(x) sin(wx)\,dx.$$

(2)
$$f(x) = \frac{i}{\pi}\int_{0}^{\infty} \overline{f(w)} sin(wx)\,dw.$$

Proof 1
By definition, we know that

$$\overline{f(w)} = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx} f(x)\,dx, \overline{f(w)} = \int_{-\infty}^{\infty} (\cos(wx) - i\sin(wx))\,f(x)\,dx,$$
$$\overline{f(w)} = \int_{-\infty}^{\infty} f(x)\cos(wx)\,dx - i\int_{-\infty}^{\infty} f(x)\sin(wx)\,dx \quad \text{Equation (a).}$$

Since the given function is odd, therefore f(x) sin(wx) is even and f(x) is an odd function. So, the first integral on R.H.S of equation (a) is zero. So, we have

$$\overline{f(w)} = -2i\int_{0}^{\infty} f(x) sin(wx)\,dx.$$

Proof 2
By definition, we know that

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx}\overline{f(w)}\,dw,$$
$$\overline{f(w)} = \frac{1}{2\pi}\int_{-\infty}^{\infty} (\cos(wx) + i\sin(wx))\,\overline{f(w)}\,dw,$$
$$\overline{f(w)} = \frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\cos(wx)\,dw + i\frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\sin(wx)\,dw \quad \text{Equation (b).}$$

By part (1)

$$2\overline{f(-w)} = -i\int_{0}^{\infty} f(x)\sin(-wx)\,dx,$$
$$\overline{f(-w)} = 2i\int_{0}^{\infty} f(x)\sin(wx)\,dx = -\overline{f(w)}.$$

The first part in the integral is odd, so the first part in the integral of equation (b) is zero. So, we have

$$f(x) = \frac{2i}{2\pi}\int_{0}^{\infty} \overline{f(w)}\sin(wx)\,dw,$$
$$f(x) = \frac{i}{\pi}\int_{0}^{\infty} \overline{f(w)}\sin(wx)\,dw.$$

4. DISCUSSION AND RESULTS

4.1. **Fourier transformation.** Fourier transformation is defined as

$$\overline{f(w)} = \mathcal{F}\{f(x)\} = \int_{-\infty}^{\infty} e^{-iwx} f(x)\,dx, \quad -\infty < w < \infty \quad \ldots\ldots\ldots\ldots (1).$$

Where f(x) is a continuous function over $-\infty < w < \infty$
The function used in Fourier transform may be real or complex, but Fourier transform in general is a complex valued function. Fourier Transformation is defined as the process in which Fourier transform is obtained.
Note: The Fourier transforms of a given function f(x) only exist if the integral on the right side of the equation converges for some value of w; otherwise, it does not exist.

4.2. **Inverse Fourier transformation.** The inverse Fourier transformation is denoted by f(x) and is defined as

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx}\overline{f(w)}\,dw \quad \ldots\ldots\ldots\ldots\ldots (2).$$

Pair of equations (1) and (2) is often called as Fourier transform pair.

Theorem 4.1
If f(x) is an even function, then

(1)

$$\overline{f(w)} = 2\int_{0}^{\infty} f(x)cos(wx)\,dx.$$

(2)

$$f(x) = \frac{1}{\pi}\int_{0}^{\infty} \overline{f(w)}cos(wx)\,dw.$$

Proof 1
By definition, we know that

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx}\overline{f(w)}\,dw = \int_{-\infty}^{\infty} (\cos(wx) - i\sin(wx))\,f(x)\,dx$$
$$= \int_{-\infty}^{\infty} f(x)\cos(wx)\,dx - i\int_{-\infty}^{\infty} f(x)\sin(wx)\,dx \quad \text{Equation (a).}$$

The second integral in equation (a) is zero because the function f(x) is an even function, therefore f(x) cos?wx is even and f(x) sin?wx is odd. So, the equation (a) becomes

$$\overline{f(w)} = 2\int_{0}^{\infty} f(x)cos(wx)\,dx.$$

Proof 2
By definition, we know that

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx}\overline{f(w)}\,dw = \frac{1}{2\pi}\int_{-\infty}^{\infty} (\cos(wx) + i\sin(wx))\,\overline{f(w)}\,dw,$$
$$= \frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\cos(wx)\,dw + i\frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\sin(wx)\,dw \quad \text{Equation (b).}$$

By part (1)

$$\overline{f(-w)} = 2\int_{0}^{\infty} f(x)\cos(-wx)\,dx,$$
$$\overline{f(w)} = 2\int_{0}^{\infty} f(x)\cos(wx)\,dx.$$

The second integral on R.H.S of equation (b) is zero because the function in second integral $\overline{f(w)}sin(wx)$ is an odd function. So, we have

$$f(x) = \frac{2}{2\pi}\int_{0}^{\infty} \overline{f(w)}\cos(wx)\,dw,$$
$$f(x) = \frac{1}{\pi}\int_{0}^{\infty} \overline{f(w)}\cos(wx)\,dw.$$

Theorem 4.2
If f(x) is an odd function, then

(1)
$$\overline{f(w)} = -2i\int_0^\infty f(x)sin(wx)\,dx.$$

(2)
$$f(x) = \frac{i}{\pi}\int_0^\infty \overline{f(w)}sin(wx)\,dw.$$

Proof 1
By definition, we know that

$$\overline{f(w)} = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx}f(x)\,dx, = \int_{-\infty}^{\infty} (\cos(wx) - i\sin(wx))\,f(x)\,dx,$$
$$\overline{f(w)} = \int_{-\infty}^{\infty} f(x)\cos(wx)\,dx - i\int_{-\infty}^{\infty} f(x)\sin(wx)\,dx \quad \text{Equation (a).}$$

Since the given function is odd, therefore f(x) sin(wx) is even and f(x) is an odd function. So, the first integral on R.H.S of equation (a) is zero. So, we have

$$\overline{f(w)} = -2i\int_0^\infty f(x)sin(wx)\,dx.$$

Proof 2
By definition, we know that

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-iwx}\overline{f(w)}\,dw,$$
$$\overline{f(w)} = \frac{1}{2\pi}\int_{-\infty}^{\infty} (\cos(wx) + i\sin(wx))\,\overline{f(w)}\,dw,$$
$$\overline{f(w)} = \frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\cos(wx)\,dw + i\frac{1}{2\pi}\int_{-\infty}^{\infty} \overline{f(w)}\sin(wx)\,dw \quad \text{Equation (b).}$$

By part (1)

$$2\overline{f(-w)} = -i\int_0^\infty f(x)\sin(-wx)\,dx,$$
$$\overline{f(-w)} = 2i\int_0^\infty f(x)\sin(wx)\,dx = -\overline{f(w)}.$$

The first part in the integral is odd, so the first part in the integral of equation (b) is zero. So, we have

$$f(x) = \frac{2i}{2\pi} \int_0^\infty \overline{f(w)} \sin(wx)\, dw,$$
$$f(x) = \frac{i}{\pi} \int_0^\infty \overline{f(w)} \sin(wx)\, dw.$$

4.3. **Tabular integration.** Tabular integration is considered a quick technique for integrating by parts multiple times in sequence. This method requires that one of the functions in f(x).g(x) is differentiable until reaches zero. Additionally we must be able to integrate the other functions each time we differentiate the first function.
Example 4.1

$$\int_1^2 4x^2 \cos(x)\, dx$$

We solve integral by using tabular integration

$$\int_1^2 4x^2 \cos(x)\, dx = \left[4x^2 \sin(x) + 8x\cos(x) - 8\sin(x)\right]_1^2 = 8.33.$$

Example 4.2

$$\int_0^1 48x \cos(x)\, dx$$

We solve integral by using tabular integration

$$\int_0^1 48x\cos(x)\, dx = [48x\sin(x) + 48\cos(x)]_0^1 = 0.83.$$

4.4. **Taylor series.** The formula of Taylor series of a real or complex valued function is defined as

$$f(a) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f'''(a)}{3!}(x-a)^3 + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n + \cdots$$

In sigma notation

$$f(a) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n$$

Where n! denotes the factorial of n and a ϵ R,C. If a=0 in Tayler series, then it is called McLaurin series.

Example 4.3 Taylor series of $f(x) = \frac{1}{x}$ at $a = 1$ can be found as

$$
\begin{aligned}
f(x) &= \frac{1}{x}, f(1) = \frac{1}{1} = 1 \\
f'(x) = \frac{-1}{x^2}, \quad f'(1) &= \frac{-1}{1^2} = -1 \\
f''(x) = \frac{2}{x^3}, \quad f''(1) &= \frac{2}{1^3} = 2 \\
f'''(x) = \frac{-6}{x^4}, \quad f'''(1) &= \frac{-6}{1^4} = -6 \\
f^{(4)}(x) = \frac{24}{x^5}, \quad f^{(4)}(1) &= \frac{24}{1^5} = 24 \\
&\vdots
\end{aligned}
$$

So, by formula of the Taylor series:

$$
f(1) = f(1) + \frac{f'(1)}{1!}(x-1) + \frac{f''(1)}{2!}(x-1)^2 + \frac{f'''(1)}{3!}(x-1)^3 + \cdots + \frac{f^{(n)}(1)}{n!}(x-1)^n + \cdots
$$

$$
f(1) = 1 - (x-1) + (x-1)^2 - (x-1)^3 + \cdots + (-1)^n(x-1)^n + \cdots
$$

$$
f(1) = 1 + \sum_{n=1}^{\infty} (-1)^n (x-1)^n
$$

4.5. **Piecewise function.** In simple, piecewise is a function in which more than formula is used for defining the output for different pieces of the domain.

Example 4.4

$$
f(x) = \begin{cases} x^2 + 1 & \text{if } x < 1, \\ 2 & \text{if } x \geq 1. \end{cases}
$$

We will encrypt the plain text by using one of the forms of Fourier transformation called Fourier cosine transformation over a piecewise function. And we solve integration for that function using tabular integration.

4.6. **Encryption by using Fourier transformation.** We use the following fixed substitution Tables for encryption of plain text into cipher text.

Example 4.5

Plain text = ”We can do ”.

By using the above Tables 1, 2, 3, we can write plain text letters as

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

TABLE 1. In small letters

A	B	C	D	E	F	G	H	I	J	K	L	M
26	27	28	29	30	31	32	33	34	35	36	37	38
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
39	40	41	42	43	44	45	46	47	48	49	50	51

TABLE 2. In capital letters

SPACE	#	$	@	=
52	53	54	55	56

TABLE 3. For some special characters

W	E	-	C	A	N	-	d	0
48	4	52	2	0	13	52	3	14

TABLE 4. Encryption table

$S_{(0,0)}$	$S_{(1,0)}$	$S_{(2,0)}$	$S_{(3,0)}$	$S_{(4,0)}$	$S_{(5,0)}$	5	$S_{(n,0)}$

TABLE 5. Encryption table

Give the numbering of the cells of above Table 3. So, the elements of Table 4 can be written as

$$\begin{array}{ccc} S_{(0,0)} = 48 & S_{(1,0)} = 4 & S_{(2,0)} = 52 \\ S_{(3,0)} = 2 & S_{(4,0)} = 0 & S_{(5,0)} = 13 \\ S_{(6,0)} = 52 & S_{(7,0)} = 3 & S_{(8,0)} = 14 \end{array}$$

Consider a function $f(x)=\frac{1}{(1-x)}$ whose Taylor series at $a=0$ is given as

$$f(x)=\frac{1}{1-x} \quad \text{and} \quad f(0)=\frac{1}{1}=1$$
$$f'(x)=\frac{1}{(1-x)^2} \quad \text{and} \quad f'(0)=\frac{1}{1^2}=1=1!$$
$$f''(x)=\frac{2}{(1-x)^3} \quad \text{and} \quad f''(0)=\frac{2}{1^3}=2=2!$$
$$f'''(x)=\frac{6}{(1-x)^4} \quad \text{and} \quad f'''(0)=\frac{6}{1^4}=6=3!$$
$$f^{(4)}(x)=\frac{24}{(1-x)^5} \quad \text{and} \quad f^{(4)}(0)=\frac{24}{1^5}=24=4!$$
$$\vdots$$
$$f^{(n)}(0)=\frac{n!}{1^n}=n!$$

By using the formula of Taylor series

$$f(a)=f(a)+\frac{f'(a)}{1!}(x-a)+\frac{f''(a)}{2!}(x-a)^2+\frac{f^{(3)}(a)}{3!}(x-a)^3+\dots+\frac{f^{(n)}(a)}{n!}(x-a)^n+\dots$$
$$f(a)=f(0)+\frac{f'(0)}{1!}(x-0)+\frac{f''(0)}{2!}(x-0)^2+\frac{f^{(3)}(0)}{3!}(x-0)^3+\dots+\frac{f^{(n)}(0)}{n!}(x-0)^n+\dots$$

$$f(a)=1+\frac{1!}{1!}(x)+\frac{2!}{2!}(x)^2+\frac{3!}{3!}(x)^3+\dots+\frac{n!}{n!}(x)^n+\dots$$
$$f(a)=1+(x)+(x)^2+(x)^3+\dots+(x)^n+\dots$$
$$\frac{1}{1-a}=f(a)=\sum_{n=0}^{\infty}x^n \quad \text{(Equation 1)}$$

Equation (1) is our desired Maclaurin series. Sequence obtained from Equation (1) is $(x)^n$ Such that n=0,1,2,3,4,5,6, . . . whose terms (a_j) are

$$x^0, x, x^2, x^3, x^4, ...$$

Multiply each plain text coefficient $S_{(i,0)}$ with each term of sequence a_j obtained from Equation(1) such that "$i=j$" then we can find the following pattern.

$S_{(0,0)}(1\cdot x^0)=$	48	$S_{(1,0)}(1\cdot x^1)=$	$4x$	$S_{(2,0)}(1\cdot x^2)=$	$52x^2$
$S_{(3,0)}(1\cdot x^3)=$	$2x^3$	$S_{(4,0)}(1\cdot x^4)=$	$0x^4$	$S_{(5,0)}(1\cdot x^5)=$	$13x^5$
$S_{(6,0)}(1\cdot x^6)=$	$52x^6$	$S_{(7,0)}(1\cdot x^7)=$	$3x^7$	$S_{(8,0)}(1\cdot x^8)=$	$14x^8$

Multiply both sides of above equations with "x".

$$
\begin{array}{llllll}
S_{(0,0)}(1 \cdot x^1) = & 48x^1 & S_{(1,0)}(1 \cdot x^2) = & 4x^2 & S_{(2,0)}(1 \cdot x^3) = & 52x^3 \\
S_{(3,0)}(1 \cdot x^4) = & 2x^4 & S_{(4,0)}(1 \cdot x^5) = & 0x^5 & S_{(5,0)}(1 \cdot x^6) = & 13x^6 \\
S_{(6,0)}(1 \cdot x^7) = & 52x^7 & S_{(7,0)}(1 \cdot x^8) = & 3x^8 & S_{(8,0)}(1 \cdot x^9) = & 14x^9
\end{array}
$$

Now, we write our outcome elements as piecewise function as follows
Now,

$$
\begin{array}{cc}
48x^1 & 0 < x < 1 \\
4x^2 & 1 < x < 2 \\
52x^3 & 2 < x < 3 \\
2x^4 & 3 < x < 4 \\
0x^5 & 4 < x < 5 \\
13x^6 & 5 < x < 6 \\
52x^7 & 6 < x < 7 \\
3x^8 & 7 < x < 8 \\
14x^9 & 8 < x < 9
\end{array}
$$

We evaluate our whole function piece wisely one by one using tabular integration.

$48x^1$

$\int_0^1 48x^1\, dx = [48x \sin x + 48 \cos x]_0^1 = 0.83$

$4x^2$

$\int_1^2 4x^2\, dx = \left[4x^2 \sin x + 8x \cos x - 8 \sin x\right]_1^2 = 0.833$

$52x^3$

$\int_2^3 52x^3\, dx = \left[52x^3 \sin x + 156x^2 \cos x - 312x \sin x - 312 \cos x\right]_2^3 = 106.84$

$2x^4$

$\int_3^4 2x^4\, dx = \left[2x^4 \sin x + 8x^3 \cos x - 24x^2 \sin x - 48x \cos x + 48 \sin x\right]_3^4$
$= 27.23688 + 295.04881 - 15.48191 - 47.72964 - 0.036184 = 259.9103$

$13x^6$

$\int_5^6 13x^6\, dx = \begin{bmatrix} 13x^6 \sin x + 78x^5 \cos x - 390x^4 \sin x \\ - 1560x^3 \cos x + 4680x^2 \sin x + 9360x \cos x - 9360 \sin x \end{bmatrix}]_5^6$
$= 45695.92952 + 360382.9185 - 31588.65418 - 140856.1317 + 7413.73359 + 9230.437773 - 162.6086 = 250115.6248$

$52x^7$

$$\int_6^7 52x^7\,dx = \begin{bmatrix} 52x^7\sin x + 364x^6\cos x - 2184x^5\sin x \\ -10920x^4\cos x + 43680x^3\sin x + 131040x^2\cos x \\ -262080x\sin x - 262080\cos x \end{bmatrix}_6^7 = 18970445.79$$

$3x^8$

$$\int_7^8 3x^8\,dx = \begin{bmatrix} 3x^8\sin x + 24x^7\cos x - 168x^6\sin x \\ -1008x^5\cos x + 5040x^4\sin x + 20160x^3\cos x \\ -60480x^2\sin x + 120960x\cos x + 120960\sin x \end{bmatrix}_7^8$$

$= 489715.99 + 30224117.41 - 3720458.615 + 15893519.95 + 139821.429$
$+ 3358130.251 - 177537.8688 - 117853.9272 + 2093.06251$
$= 19970445.78$

$8x^9$

$$\int_8^9 8x^9\,dx = \begin{bmatrix} 8x^9\sin x + 72x^8\cos x - 576x^7\sin x. \\ -4032x^6\cos x + 24192x^5\sin x + 120960x^4\cos x \\ -483840x^3\sin x + 1451520x^2\cos x + 2903040x\sin x \\ +2903040x\cos x \end{bmatrix}_8^9$$

$= 335411356.3 + 1865001826 - 262859932.7 - 1069710755 + 113142949.2$
$+ 293217345 - 2070065.65 - 24132389.73 + 855018.9524 - 7489.053998$
$= 1230217271$

Similarly, we apply tabular integration to all parts and we obtain the following results

$48x^1$	$0 < x < 1$	0.83
$4x^2$	$1 < x < 2$	8.33
$52x^3$	$2 < x < 3$	106.84
$2x^4$	$3 < x < 4$	259.910
$10x^5$	$4 < x < 5$	0
$13x^6$	$5 < x < 6$	250115.6241
$52x^7$	$6 < x < 7$	18970445.70
$3x^8$	$7 < x < 8$	19979445.78
$14x^9$	$8 < x < 9$	1230217271

$S_2 = 0.83, 8.33, 106.84, 259.910, 0, 250115.6241, 18970445.70, 19979445.78, 1230217271.$
Now we can obtain
$S_3 = 0.83e+(-2)8.33e+(-2)106.84e+(-3)259.910+(-8)250115.6241e+(-2)18970445.70e+(-2)19979445.78e + 1230217271e.$
Now we can obtain sequence s_3 have the form

$A_0 = 83$
$A_1 = 833$
$A_2 = 10684$
$A_3 = 259910$
$A_4 = 0$
$A_5 = 2501156241$
$A_6 = 1897044570$
$A_7 = 1997944578$
$A_8 = 1230217271$
Now we solve the all co-efficient under mod (57) by the formula.
$A_n = 57k_n + R_n \pmod{57} \quad n = 0, 1, 2, ...$
$A_n = 57k_n + R_n \pmod{57}$
$A_0 = 57(1) + 26 \pmod{57} \quad K_0 = 1,\ R_0 = 26$
$A_1 = 57(14) + 35 \pmod{57} \quad K_1 = 14,\ R_1 = 35$
$A_2 = 57(187) + 25 \pmod{57} \quad K_2 = 187,\ R_2 = 25$
$A_3 = 57(4559) + 47 \pmod{57} \quad K_3 = 4559,\ R_3 = 47$
$A_4 = 57(0) + 0 \pmod{57} \quad K_4 = 0,\ R_4 = 0$
$A_5 = 57(4387993) + 23 \pmod{57} \quad K_5 = 4387993,\ R_5 = 23$
$A_6 = 57(3378143) + 98 \pmod{57} \quad K_6 = 3378143,\ R_6 = 98$
$A_7 = 57(35035869) + 45 \pmod{57} \quad K_7 = 35035869,\ R_7 = 45$
$A_8 = 57(21582759) + 8 \pmod{57} \quad K_8 = 21582759,\ R_8 = 8$

1	14	187	4559	0	4387993	33281483	350335869	21582759

TABLE 6. Key Table Ki

26	35	25	47	0	23	48	45	8

TABLE 7. Key Table Ri

Plain text = ”we can do”.
Cipher text = ”AJzVaxWTi”.

4.7. **Decryption process.** For the decryption of cipher text into plain text, follow the following steps:

(1) Use Table 3.1, 3.2, 3.3 to write cipher text alphabets into cipher coefficients as $S_{(0,n)}$ where n = 0,1,2,3, . . . , 44.
(2) By using Table Ri and Table Ki, write $S_{(0,n)}$ in the form of A_n using the formula $A_n = 57(K_n) + S_{(0,n)}$ where n = 0, 1, 2, 3, . . . , 44.
(3) Write S_3 using these coefficient.
(4) After performing backward steps on S_3 we can easily find S_2.
(5) Apply inverse Fourier transformation and find the original ”piecewise function”.
(6) Divide all terms by ”x”.

(7) Write plain text coefficients $_{(n,0)}$ and then by using Tables 1-5, convert them into Plain text alphabetical.

5. STATEMENT OF NOVELTY

The process of protecting information by encrypting it into an unreadable format is called ciphertext. Decryption of the message and its conversion into text is limited to those who possess the secret key. Encrypted messages can sometimes be broken by crypt-analysis, also called cipher cracking, but modern cryptographic techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more widespread, cybersecurity is becoming increasingly important. Encryption is used to protect email messages, credit card information, and company data. Pretty Good Privacy is one of the most popular encryption schemes used on the Internet because it is both effective and free. Cryptographic systems can be broadly categorized into symmetric key systems that use a single key held by both the sender and the receiver, and public key systems that use two keys: a public key known to all and a private key that only message recipients use. In this paper, our research concept of encoding and decoding a message using Fourier transform and finite state machine.

6. DISCUSSION

Protection of personal data, knowledge, and hidden messages is the main objective of this study. This study ensures the protection of any type of message that individuals wish to communicate. Messages can be encoded using the Fourier algorithm, which includes small letters and capital letters, as well as spaces. This approach offers several advantages for military and government communication without any doubt, this approach has several advantages. In this article, we have presented "The Role of Fourier transformation in cryptography" using the Fourier Transformation. Various types of Cryptography and ciphers [9, 14, 17, 20] are employed for this purpose we have also discussed the implementation of the Taylor series and Fourier Transformation in real life. The scenarios as well as approaches used in the past and their strategies. Some techniques used in past and their founders are discussed in detail in this course.
Fourier transformation offers unique advantages in cryptography due to its ability to analyze and manipulate signals in the frequency domain. It has applications in cryptanalysis, steganography, homomorphic encryption, and potentially post-quantum cryptography. However, it is essential to consider the computational complexity and sensitivity to noise when applying Fourier transform in cryptographic contexts.

7. CONCLUSION

This study refers to some fundamental concepts of Fourier transformation, inverse Fourier transformation, and Taylor series. It clarifies some essential features and regular theorems. Encryption [6, 7, 8, 13, 18, 23] tables and decryption have been expanded according to mod 57. These table play an important role in coding and decoding hidden messages. Some basics are also discussed for the results of simple and exponential functions [11, 12, 15]. The methodology for this course is established through the use of Fourier transformation and series form of simple and exponential functions, as well as the use of Fourier transformation for coding and decoding necessary functions in order to keep messages secret. This work is expanded by taking mod 57 and using the reciprocal Fourier transformation in decryption. This also covers the space bar that is also required to keep it hidden. This algorithm provides security from hackers. This study aims to dive deeply into the mathematical foundations and applications of Fourier Transformation in encryption and decryption processes, specifically with the use of modular arithmetic (mod 57).

The focus on transforming messages into different forms using Fourier and Taylor series highlights how mathematical techniques can enhance cryptographic security. The incorporation of coding tables for encoding and decoding hidden messages provides a practical approach to managing data confidentiality.

Additionally, discussing the inverse Fourier Transformation and its role in decryption emphasizes the importance of useful reversible processes in cryptography, ensuring that encrypted information can be accurately restored.

It's interesting to see how such mathematical concepts can be applied to create algorithms that secure messages against unauthorized access.

Acknowledgments. All authors are thankful to those who supported this work.

Conflicts of Interest. The authors declare that they have no conflicts of interest to report regarding the present study.

Motivation and Reference Work. Inspired by the article "Research on Various Cryptography Techniques written by Yahia Alemami, Mohamad Afendee Mohamed, and Saleh Atiewi".

Data Availability. All data used are included inside the manuscript.

Statement of Contribution. Muhammad Haroon Aftab: Integrated data, formatting, data analysis, editing and proofreading.
Shakila Rehman: Wrote original drat, methodology and computations.

References

[1] R. P. Adhie, Y. Hutama, A. S. Ahmar, and M. I. Setiawan. *Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC)*, In Journal of Physics: Conference Series **954**, no. 1(2018), 1-9.

[2] I. Anshel, M. Anshel, and D. Goldfeld. *An algebraic method for public key cryptography*. Math. Res. Lett. **6**, no. 3(1999): 287-291.

[3] G. R. Blakley. *Twenty years of cryptography in the open literature*. In Proceedings of the IEEE Symposium on Security and Privacy (Cat. No. 99CB36344), (1999): 106-107.

[4] J. Buchmann. *Introduction to cryptography*. springer, New York 335, (2004).

[5] D. Davies. *A brief history of cryptography*. Information Security Technical Report **2**, no. 2(1997): 14-17.

[6] Q. DuPont, *Cryptocurrencies and blockchains*, John Wiley and Sons, (2019).

[7] H. Gupta, and V. K. Sharma. *Multiphase encryption: A new concept in modern cryptography*. International Journal of Computer Theory and Engineering **5**, no. 4(2013): 638.

[8] A. I. Hussein, A. T. MaoLood, and E. K. Gbashi. *Ntru sss: a new method signcryption post quantum cryptography based on shamir's secret sharing*. COMPUT MATER CON **76**, no. 1(2023): 753-769.
[9] K. Jonathan, and Y. Lindell. *Introduction to modern cryptography*. CRC press, (2020): 1-512.
[10] I. Y. Jung and H. Y. Yeom. *Enhanced security for online exams using group cryptography*. IEEE transactions on Education **52**, no. 3(2009): 340-349.
[11] H. Khalil, R. A. Khan, M. H. Al-Smadi, A. A. Freihat. *Approximation of solution of time fractional order three-dimensional heat conduction problems with Jacobi Polynomials*. Punjab Univ. J. Math. **47**, no. 1(2020).
[12] S. Khan, M. Gulistan, H. A. Wahab. *Development of the structure of q-rung orthopair fuzzy hypersoft set with basic operations*. Punjab Univ. J. Math. **53**, no. 12(2022).
[13] Y. Li, H. Kan, J. Peng, and L. Zheng. *Cryptographic functions with interesting properties from CCZ-equivalence*. Cryptogr. Commun. (2023).
[14] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*, CRC press. (2018): 1-794.
[15] R. Navalakhe, H. Atre. *IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS USING MOORE MACHINE AND RECURRENCE MATRIX*. Punjab Univ. J. Math. **55**, no. 3(2023).
[16] A. Papoulis. *A new method of inversion of the Laplace transform*. Q. Appl. Math. **14**, no. 4(1957): 405-414.
[17] A. M. Qadir, and N. Varol. *A Review Paper on Cryptography*. International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, (2019): 1-6.
[18] M. Ragab, and E. B. Ashary. *Metaheuristic lightweight cryptography for security enhancement in internet of things*. COMPUT MATER CON **72**, no. 2(2022): 3009-3023.
[19] P. Refregier, and B. Javidi. *Optical image encryption based on input plane and Fourier plane random encoding*. Opt. Lett. **20**, no. 7(1995): 767-769.
[20] S. D. Robert, and M. Paterson. *Cryptography: theory and practice*. CRC press, (2018): 1-611.
[21] S. Saeednia. *how to make the Hill cipher secure*. Cryptologia **24**, no. 4(2000): 353-360.
[22] B. Schneier. *Cryptography: The importance of not being different*. Computer **32**, no. 3(1999): 108-109.
[23] Wang and X. Bao. *Cryptanalysis of an image encryption algorithm using Chebyshev generator*. Digit. Signal Process. **25**, (2014): 244-247.