Republic of Iraq

Ministry of Higher Education and Scientific Research
University of Babylon
College of Sciences for Women
Department of Computer Sciences

Hybrid Encryption Model Based on Molecular and Microfluidic Techniques

A Thesis

Submitted to the Council of College of Science for Women, the University of Babylon in a Partial Fulfilment of the Requirements for the Degree of Master in Science\ Computer Sciences

By

Hiba Safaa Hashim

Supervised By

Dr. Sahar Adil Kadhum **Dr. Ali Yakoob Al-Sultan**

2023 A. D. **1444 A. H.**

سورة البقرة الآية: ٣٢

Supervisor Certification

I certify that this thesis entitled

Hybrid Encryption Model Based on Molecular and Microfluidic Techniques

written by

"Hiba Safaa Hashim"

was prepared under my supervision at College of Sciences for Women as a partial fulfillment of the requirements for the degree of a Master's in Computer Sciences.

Signature:	***Signature:***
Name: Dr. Sahar Adil Kadhum	***Name: Dr. Ali Yakoob Al-Sultan***
Date: / / 2023	***Date: / / 2023***

Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled* "Hybrid Encryption Model Based on Molecular and Microfluidic Techniques"** ***for debate by the examining committee.

Signature:
Name: Asst.prof.Dr Saif Mohmood Alalak
Date: / / 2023
Address: University of Babylon/College of Science for Women

Acknowledgements

First of all, I thank God who inspired me with patience and strength to complete this study.

It is not easy except for what God makes easy.

I would like to express my sincere thanks and appreciation to the Supervisor

Dr. Sahar Adill Kadim and Dr. Ali Yakoob Al-Sultan

To guide and follow up with me and provide important tips and suggestions to improve this study. Without them, I would not have completed this thesis. I learned a lot from them on this journey of research. I am really grateful to them.

Dedications

To my great creator, dear God

To the first teacher of mankind, the prophet Mohammed, may God bless him and his family and grant them peace.

To my intercession with God in this world and the hereafter, the pure imams, peace be upon them.

To my present absent father, how I longed to see the fruit of this harvest in your kind eyes. Peace be upon your pure soul.

To the fountain of patience that mortgaged her health to see us alone today... my honorable mother

To those who supported me and encouraged me with all love and patience.....my husband and children

To those who wish happiness and success for me from the bottom of their hearts without any compensation ... my dear brothers and sisters.

To all my dear loyal friends

I offer you that humble work .....

Hiba

Abstract

Local networks and the Internet increase day by day, and a large amount of information is transferred across these networks every day resulting in a dramatic increase in the information security threats. Therefore, it was necessary to use the techniques that ensure the security and the confidentiality of the transferred information. For these reasons, many techniques proposed to protect such information such as Cryptography and Information hiding to improve the security of transferring the information over the internet.

Recently, the bio-molecule discipline has entered the security direction to play a distinct role in this field using DNA cryptography. It promising field in information security. It combines classical solutions in cryptography with the strength of the genetic material. By introducing DNA into the common symmetric key cryptography, it is possible to benefit from the advantages of the classical cryptosystems and solve some of its limitations. There are different ways how DNA can be used to secure information content. It is about using the biological medium of DNA for storing and hiding data. Secret information can be placed in microscopic size of DNA and hidden among a great amount of other DNA structures. Biomolecular computation is possible with specially designed DNA structures. Valuable parts of this type of computation are self assembling property of DNA molecules and parallel computations.

This thesis proposed a new hybrid symmetric stream cipher encryption algorithm based on microfluidic technology and DNA sequences.The proposed method includes three phases (key generation, encryption, decryption process). First phase is the key generation procedure based on nonlinearity behavior of

microfluidic technology, composed three steps:(Key pad generation, Seed key selection, Key expansion)

The second phase is the encryption procedure to encrypt the message in DNA sequences with XOR operation to get a strong, secure and relatively unbreakable cipher text in DNA format.

The third phase is decryption procedure to retrieve the original message by reversing the encryption processes.

The experimental results of proposed system have proved the efficiency of our method in achieve robust and multilevel security dimension through a set of metrics such as (avalanche effect(78.39 %, 65.13 %, 78.28 %), encryption time(0.1043, 0.2078, 0.3022), decryption time(0.1033, 0.2056, 0.3077), throughput(9.1046, 8.8899, 6.9351), BER(0.2086, 0.4011,0.5597)) for (1KB,2KB,3KB) file size respectively.

Table of Contents

Table of Figures

List of Tables

List of Algorithms

List of Abbreviations

Abbreviations	Meaning
BER	Bit Error Rate
DNA	Deoxyribo Nucleic Acid
DES	(Data Encryption Standard) Algorithm
LFSR	Linear Feedback Shift Register.
NIST	National Institute of Standards and Technology
NPCR	Number of Pixels Change Rate
OTP	One Time Pad
PRNGs	Pseudo random Number Generators
RNA	Ribo Nucleic Acid
RSA	(Rivest–Shamir–Adleman) Algorithm
TRNGs	True number generators
UACI	Unified Average Changing Intensity

Chapter One
General Introduction

1.1 Introduction

Information security is one of the most important fields that has been gaining more attention for data protection, privacy preservation and data leakage prevention[1]. Security in data communication is required when message transfer between sender and receiver is needed to be kept confidential [2]. Data hiding and cryptography, two ideas that are closely connected to one another, are the approaches that see the most widespread use in the disciplines of computer security and communication security respectively [3]. The development and use of these systems are distinct, despite the fact that the two sets of protocols share the objective of ensuring the privacy and integrity of data[3].

Cryptography is the art and science of hiding important and secret information from being infringed upon by unauthorized persons. It is all about protecting and safeguarding information from cyber criminals or anyone else other than the intended recipient. Cryptography enables people to communicate on the Internet, transferring crucial and confidential information securely. It helps users and institutions to cipher and decipher hidden messages into codes, so information can be transmitted safely. Cryptography is initiated by encryption and decryption keys. The process of coding and transformation of plain text into the unreadable format is called encryption; while the process of decoding and converting the unreadable text to readable information using a special digital key is called decryption. the purpose of cryptography is to protect information, email, credit card details and other personal data transmitted across a public network[4].

Cryptography is changing the apparent features of the text sent by one of the many encryption algorithms, so that it is difficult to understand after it is encrypted, except by the sender and the receiver [5].

Given the importance of the keys used in encryption as a key part in the strength of the algorithm and increase its security in most encryption algorithms, thus generating the key in many research is the most important part in data encryption and its importance lies in the non-duplication of keys to ensure better results and theoretically impossible to break.[6] The key resists cryptanalysis whenever the key is strong as it resists even against the attacker who detects all system information related to the creation or verification of the encryption key [7].

Most of the existing encryption algorithms depend on the generation of keys on mathematical bases, on the other hand, there are counter methods for breaking keys and mathematical foundations based on. Therefore, the process of searching for a new methods to generate encryption keys is being worked on by introducing new scientific trends and concepts, including the use of biology and Chemistry to take advantage of the methods and techniques that characterize it to be employed it in several security directions, including the generation of keys that are characterized by the difficulty in predicting keys and complexity, where vital information is characterized by its data density and multiple techniques and this helps in building complex and unbreakable encryption key .As for the chemical aspect, through the use of the microfluidic technique, which adopts different entry methods for liquids with non-linear behavior. Since the nonlinear fluid behaviors are not fully understood by humans. In this research, we use the microfluidic chip technique to generate a set of random seed keys. Since there is no method of mathematical analysis for predicting nonlinear fluid behaviors, it is not affected by the attack of mathematical analysis. This approach gives new insights into information security and we hope that it is a new promising path. The main target of this work is to propose a new algorithm for encrypting data using key features of DNA computing and OTP cryptography.

1.2 Related Works

Encryption using DNA encoding can significantly improve the security of the cryptographic solution. A large volume of published studies describes the role of DNA in cryptography.

In 2018 Animesh Hazra, et al[8]: proposed a novel technique built on the combination of DNA nucleotides, symmetric-key cryptography, and the XOR operation. This method is adaptable . An additional layer of security is provided by the substitution technique and XOR operation. According to mathematical study, the key can be figured once per million tries. This method's ease of use and effectiveness are additional benefits.

In 2018, Asoke Nath, et al. [9]: proposed an encryption system based on DNA sequence. In this system the plain text is being divided into bits and multiple mathematical functions have been used on it and then converted to DNA form.In the present paper the authors aims at converting the plaintext into a form unreadable form and then it can be readily transferred across the web and decrypted at the recipient side only by authorized people. It provides an algorithm to encrypt, decrypt or transfer encrypted files without compromising with the integrity and privacy of critical information.

In 2019, Lalit Mohan, et al [10]: An improved DNA Based Security Model using Reduced Cipher text Technique. uses DNA-based multi-layer encryption with a 128-bit key. It also includes a round key selection technique, a random series of DNA-based coding and modified DNA-based coding, followed by a unique method of substitutions. This technique increases the size of the cipher text by 33% as compared to conventional DNA and non DNA based algorithms, It also takes less time to encrypt and decrypt large file size data.

In 2019 Ragavan, M,et al.[11]: Proposed a new symmetric block cipher DNA-based encryption technique, and they utilized the DNA sequence to generate a random and strong secret key, which is rigid to be broken by attackers. Their proposed algorithm is composed of substitution and transposition operations. They evaluated the effectiveness of their proposed DNA based encryption algorithm from encryption time, key size, and proportion of alterations prospective compared with two traditional encryption algorithms, namely: DES and AES.

In 2020 Jieyu Zheng ,et al.[12]: Proposed a new symmetric block cipher DNA-based encryption technique, and they utilized the DNA sequence to generate a random and strong secret key, which is rigid to be broken by attackers. Their proposed algorithm is composed of substitution and transposition operations. They evaluated the effectiveness of their proposed DNA based encryption algorithm from encryption time, key size, and proportion of alterations prospective compared with two traditional encryption algorithms, namely: DES and AES.

In 2020 , B.Mohan Kumar, et al. [13]: proposed a DNA-based encryption system that encrypts messages using both the process of binary coding and the creation of arbitrary keys. It is frequently used by both institutions and individuals to protect their information from thieves and hijackers during information transmission. Data security and integrity are provided during the data transmission procedure. This algorithm uses memory effectively as well.

In 2021 Adélaïde Nicole Kengnou Telem et al [14] presents a new image encryption algorithm based on 3D chaotic system and deoxyribonucleic acid (DNA) coding. It uses two keys, an external one of 128 bits long and an internal one of 64 gray values coming from the plain image. The initial conditions come from the two keys and vary from one line of the image to the

other and from one image to the other and consequently the sequences of substitutions too. Correlation coefficients, entropy information.

In 2021 Omar Fitian Rashid[15]: proposed a cryptography system based on DNA sequences by convert plain text to DNA characters.The DNA characters are converted to RNA sequences, then RNA sequences are converted to the amino acid, where this sequence is considered as cipher text to be sent to the receiver. Performance evaluation is calculated based on encryption time and decryption time.

In 2023 Pramod Pavithran et al [16]: proposes a cryptosystem based on DNA cryptography and finite state machines, in the proposed scheme, a randomly generated DNA-character conversion table is used to convert the characters in the plaintext to a DNA sequence. Then, the DNA sequence is converted to a binary string and many EXOR operations are performed between the binary string and a 256-bit secret key. The binary string is encoded as a DNA sequence and input to finite state machines,. These machines translate the DNA sequences to new DNA sequences, and finally, the ciphertext is generated.

The following summarize the related works (table 1.1))

Table (1.1) Summary of Related Work

Author name	year	data	Technique	Type	Performance
Animesh Hazra et al.	2018	Text	XOR ,DNA coding	Symmetric	Frequency test, frequency test within a block, and runs tests
Asoke Nath et al.	2018	Text	XOR, DNA coding	Symmetric	----------
Lalit Mohan Gupta	2019	Text	XOR, DNA coding	Symmetric	Execution time and cipher text file size
Ragavan M,et al.	2019	Text	AES module in crypto tool is used for encryption and decryption process.	Symmetric	Encrypted and decrypted processing time, entropy values
Jieyu Zheng et al.	2020	Image	2D logistic sine chaotic map, DNA coding	Symmetric	NIST test, information entropy
Mohan Kumar	2020	Text	DNA coding	Symmetric	----------
Omar Fitian Rashid	2021	Text	DNA and RNA sequence	Symmetric	Encryption and decryption time
Adélaïde Nicole Kengnou Telem	2021	Image	DNA coding , Adélaïde Nicole Kengnou Telem		NCPR, UACI, Correlation coefficients
Pramod Pavithran1 et al	2023	Text	DNA cryptography and finite state machines.	Symmetric	(NIST) test suite, avalanche
Proposed system			Microfluidic technique, logistic map, DNA coding, XOR operation	Symmetric	(NIST)test suit,encryption and decryption time, throughput, BER, avalanche effect, histogram

1.3 Problem Statement

Today, in the age of computerization, we are facing increasing risk of having our intellectual property compromised, and falling victims to cheating, fraud and impersonation. Therefore, we need strong cryptography to protect us from these criminals [17].

There are many encryption algorithms that rely on the mathematical principle, and on the other hand there are cryptanalysis technologies for breaking the coding techniques and ciphering. Therefore, the need to develop

and invent new protection technologies are continuous process to secure information from unauthorized access. From the view of coding a ciphering key.

Where the ciphering keys is built on a mathematical base. Theses bases can be broken, and therefore the possibility of accessing the encryption keys and finding the explicit text of data and information, so the need to find new methods that are not dependent on the mathematical aspects has become very necessary.

Therefore, this thesis introduces a nonmathematical method for generating the cipher keys. which employ the chemical technique used in the microfluidic chip, bio information and chaotic system to enhances the power of encryption while also providing increased complexity and security.

1.4 Objectives

The aim of this thesis is to adapt a new method to generate randomly encrypted keys, given that random keys are difficult to break and guess. The proposed method relied on a cipher key that goes through two stages of randomness :

a. Using of microfluidic technology to generate random seed keys by exploiting the nonlinear behavior.

b . To increase the randomness of ciphering key a logistic chaotic map is integrated with the seed key to obtain another level of security that is difficult to break .

1.5 Thesis Layout

The structure of this thesis consist of five chapters:

Chapter One: Entitled "General Introduction" presents an introduction to information security, Related Works, Problem Statement and Thesis Objectives.

Chapter Two: presents the basic principles of theoretical background techniques used in this thesis such as cryptography techniques, microfluidic technique ,DNA technique , DNA molecular , chaotic maps , logistic map .

Chapter Three: Presents the theoretical proposal algorithm.

Chapter Four: presents the implementation and results of the proposal system.

Chapter Five: summarizes the conclusions and future research suggestion work**.**

Chapter Two
Theoretical Background

2.1 Introduction

This chapter explains the basic concepts of the theoretical background that this thesis deals with. It focuses on: security principles, Cryptography techniques, molecular computation, DNA sequence, microfluidic technique, chaotic system, logistic map, and possible attacks on encryption algorithm.

2.2 Security Principles

The Internet plays an important role in day-today life. The people can transfer large amount of data that are critical and consume large amount of time through the internet such as Email, banking transaction and online purchase. But due high exposure they are susceptible to being heavily attacked or become attractive targets for attackers. This means that they require special care to make this information secure and resilient against security treats [19].

The information security triad is based on three main aspects availability, integrity and confidentiality. The goal of cryptography is to cover the major portion of integrity and confidentiality in different application such public and private algorithms, Key distribution management for confidentiality of stored and transmitted data, digital signature for authenticity of electronic transactions activities and for non-repudiation conformities [20].

As relation between user and internet is increasing rapidly the chances of theft also increase, so there are more requirements to secure the data transmitted over different network using different services. To provide the security to the network and data different encryption methods are used. By using the security mechanism we have to protect data from unintended or unauthorized access, change or destruction. Cryptography is the art of secret writing to hide information

secret or keeping message secure. A secure network must have integrity, so that all of the information stored is always correct and protected [21].

Cryptography Techniques

Encryption techniques is the only solution through which information can be secured [22].

The idea of cryptography enables information to be transferred in a safe format so that only the recipient may retrieve this information. Continuous research is now being done on new cryptographic methods. However, identifying the precise algorithm is quite challenging [23]. Modern encryption techniques concentrate on creating encryption algorithms (ciphers) that are difficult for an adversary to crack due to computational complexity and consequently cannot be cracked by a practical approach [24].

A- Encryption Algorithms

Encryption algorithms are classified into two groups: Symmetric-key (also called secret-key) and Asymmetric-key (also called public-key) encryption. As shown in figure (2.1)

- **Symmetric Encryption**: the sender and recipient share a private key known only to both of them. The same key is used for encryption and decryption. The most commonly used symmetric algorithms are AES (Advanced Encryption Standard), Cha. Blowfish, and IDEA (International Data Encryption Algorithm) , Symmetric encryption schemes are usually faster than public key counterparts and thus are preferred for encrypting big data [25]. Symmetric encryption algorithms are categorized into: block and stream ciphers.

- **stream cipher:** is an important branch of symmetric cryptosystems, which takes obvious advantages in speed and scale of hardware implementation, data is encrypted byte by byte and sometimes even bit by bit, it is suitable for using in the cases of massive data transfer or resource constraints, and has always been a hot and central research topic in cryptography.

- **Block ciphers**: convert data in plaintext into cipher text in fixed-size blocks. The block size generally depends on the encryption scheme and is usually in octaves (64-bit or 128-bit blocks). If the plaintext length is not a multiple of 8, the encryption scheme uses padding to ensure complete blocks [26].

- **Asymmetric Encryption**: two keys are used: the first one is made publicly available to senders for encrypting plaintext while the second key is kept secret and is used by the receivers for decrypting the cipher text [25]. Because asymmetric encryption techniques are 1000 times slower than symmetric encryption, they cannot be used to encrypt large amounts of data. In order to attain the same level of security as symmetric encryption, asymmetric encryption needs a stronger key [27].

- **Hash Function**: This type of cryptography does not require any digital key as it utilizes a fixed length hash value encrypted into the plain text. The purpose of the hash key is to make sure that the original information is not tampered with. This is a one-way encryption. It uses algorithms to facilitate communication. The hash key normally provides a digital fingerprint, making sure that the file is not corrupted or infected with a virus. The hash key also helps computer administrators to encrypt passwords Cryptographic hash functions have another property that it is very difficult to find two different messages that produce the same message digest. To provide the data integrity and data authentication, if a message digest of any

information is changes, then the file itself has changed. Hash function used for key generation in Symmetric and Asymmetric Key Cryptosystems. [28]

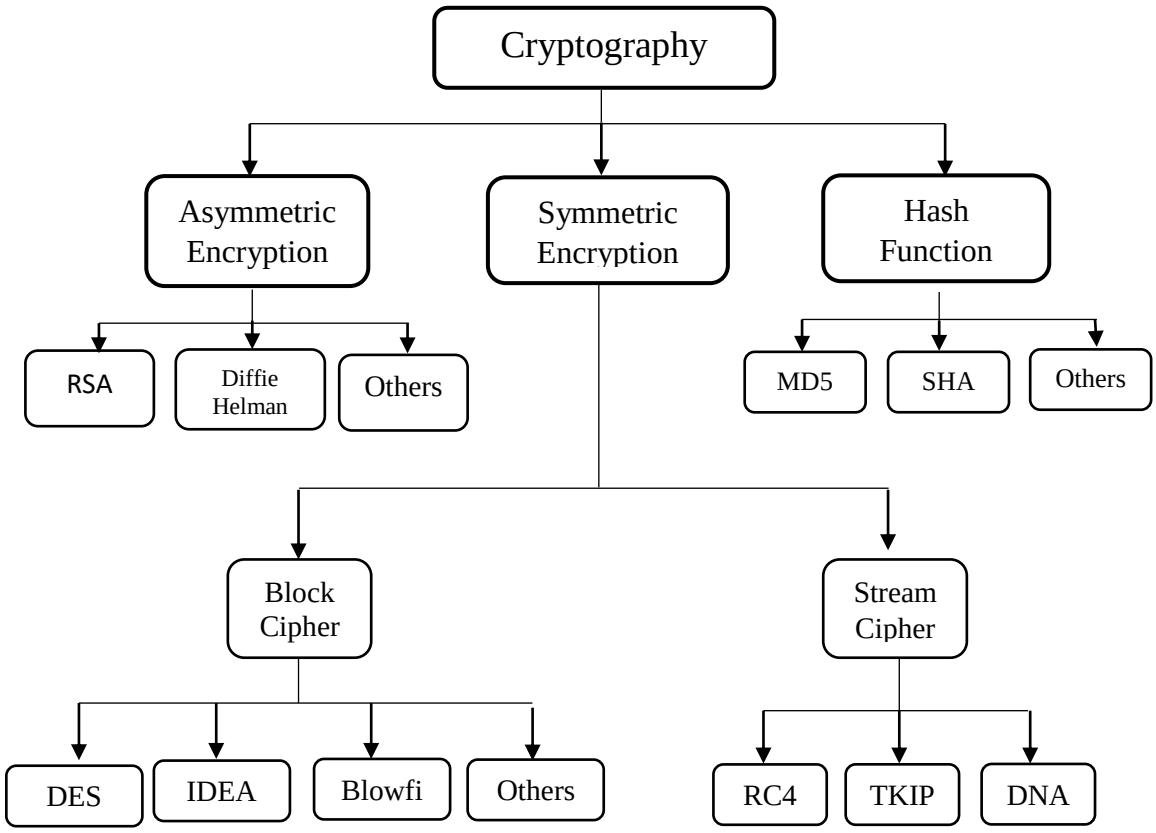


Figure (2.1): Classification of Encryption Methods [29] .

B- Encryption Key

A key is a numeric or alpha numeric text or may be a special symbol. The key is utilized when the cipher text is being decrypted and when the plain text is being encrypted. The choice of key in cryptography is crucial since it directly affects the security of the encryption technique. The strength of the encryption technique depends on the initialization vector, the length of the key, and how they all interact[30].

The strength of the encryption method and the secret of the key determine how secure encrypted data will be. The key is a component of the information in

cryptography that specifies the practical algorithm that will produce the desired cryptographic encryption. The method does not produce a result in the absence of the key. In order to prevent the key from being guessed, keys must be generated at random and with a large enough universe [31].

The process of creating keys for cryptographic systems is known as key generation. Strong cryptographic modules were required for the generation of cryptographic keys. The module that generates the key must produce the random numbers needed for key generation. The security level (randomness) that a key can offer is dependent upon the method that is utilized [31].

True random numbers, pseudo-random numbers, and quasi-random numbers are the three main categories of random numbers.

- True random numbers are derived from physical sources and do not need a seed, which is a starting sequence. They shouldn't have a correlation pattern or period, as expected. TRNGs are commonly used in cryptology, which are due to unpredictability and lack of re-production. In addition, they have unique statistical features. TRNGs have some disadvantages such as slowness, high cost and dependency on hardware

- Pseudo random number generators, produces number sequence deterministic. The main feature of pseudo random number generators is the seed value for initializing the pseudo random number generator equation, which the selection of the seed value should be done in such a way as to increase the security and avoid creating correlations in the generated sequence [32].

PRNGs used in the cryptographic system should meet a set of conditions. For example, generated pseudo-random sequences must have a long period, high

performance in fast execution, optimal memory consumption and unpredictable [32].

Special procedures are used to generate quasi random numbers, which are evenly dispersed within a unit-square or unit-cube [33] . With the use of current, highly sophisticated computing devices, hackers may now simply break the key. Strongly encrypted data that cannot be decrypted by cryptanalysis is currently needed [34].

2.3 DNA Molecular Cryptography

Since the Feistel cipher, DES (which was inspired by the Feistel cipher), MD5, and other contemporary cryptography encryption techniques have already been cracked[35]. In order to protect data, new encryption methods directions are being pursued [35] .

DNA cryptography has been identified as a new, potential trend in encryption with the development of the DNA computing area. Based on the characteristics of DNA, it is possible to improve the security and dependability of data. Although there isn't a clear connection between cryptography and biological genetic molecules in the real world, combining these two ideas has the potential to do wonders for the data security industry. The use of biological and arithmetic activities independently or in combination can be used to create DNA cryptography [36].

The benefits of DNA computing over conventional computing can be credited for the rising popularity of DNA cryptography, such as :-

- Parallel processing: 1026 operations/sec
- Data capacity: 2.2 Exabyte per gram

- Imperishable storage[37]

2.3.1 DNA Computing

DNA computing is a brand-new field that is currently growing. DNA cryptography began with the development of DNA computing. To solve a difficult computer problem, L. Adleman created DNA computing in 1994 [38].

Adleman set the foundation of the research in the field of bio computing. Many researchers were inspired to use DNA to address challenging issues in various axes of computer science by the immense parallelism and density of information that this molecule possesses, as well as the outcomes of Adleman's experience [39].

For instance, storing information in DNA molecules enables the information density of about 1 bit per nanometer. The information density of videotape, a type of conventional storage medium, is roughly 1 bit per 10 nanometers. This shows that DNA molecules have a higher information density than conventional storage media [40].

2.3.2 DNA Structure

DeoxyriboNucleic Acid (DNA), which has a double helix structure, is used to store the genetic material for every living thing, including humans and tiny viruses. It also goes by the name "information carrier" and is made up of a lengthy polymer of nucleotides, which are tiny units. Three elements make up more nucleotides: a nitrogenous base, a sugar with five carbons, and a phosphate group.

Adenine, Thymine, Cytosine, and Guanine (A, T, C, and G) are the four bases that make up the nitrogenous base, which is used to store all of the intricate information about organisms. While Thymine and Cytosine are referred to as pyrimidines, Adenine and Guanine are purines [41]. as shown in Figure (2.2).

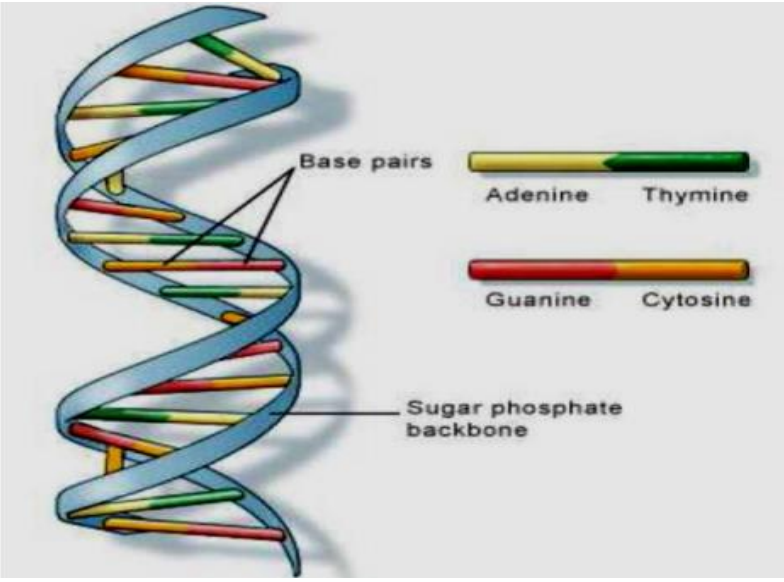


Figure (2.2): The Structure of Part of a DNA Double Helix [42]

Data absorption and transmission have been the primary uses of DNA for millions of years. DNA contains information that is handed down across generations. All human's biological characteristics are determined by new proteins that are created by the cell under the direction of the DNA, which copies this information and preserves it for billions of years. Therefore, it might consist of 10 trillion little DNA molecules [43].

2.3.3 DNA Coding

DNA can be represented by the four letters A, C, G, and T. It is simple to convert this alphabet to the binary alphabet (A – 00, C – 01, G – 10, T - 11). As a result, DNA is a versatile method of information storage. In the subject of biomolecular computing, the ability of complementary DNA nucleotide bases

(A-T, C-G), known as base pairs, to hybridize is used as a key component of computations[44]. There are eight rules for coding DNA As shown in the table (2.1) [45].

Table (2.1) : DNA encoding / decoding rules [45]

DNA bases	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

2.4 Microfluidic Concept

Microfluidics relates to the design and study of devices that move or analyze the tiny amount of liquid, smaller than a droplet. Micro channels in microfluidic devices range in size from submicron to a few millimeters. Consequently, a very small volume of liquid can be processed or seen [46].

In-depth uses for microfluidic chips can be discovered in chemical and biological studies. Numerous of these chips include elements like cells, microbeads, or droplets.

Computer-based simulations of microfluidics have gained importance as the variety of microfluidic devices has increased [47].

Although no microfluidic system has concurrently studied nonlinear and reversible fluid flow dynamics, using microfluidic devices offers a way to do so [48].

The ability to carry out a number of fundamental fluidic operations must be integrated onto a single platform in a microfluidic device. The mixing and separating processes are possibly the most crucial. The issue is how to effectively homogenize two species carried by a flow in the absence of turbulence, which significantly speeds up mixing processes in large-scale systems. Contrarily, in the case of (b), the issue is how to avoid the various species present in a flow from interacting with one another and lessening the effectiveness of the separation mechanism. Ironically, both issues in microfluidics are challenging [49].

There are several Advantages of Microfluidics :

1- Low sample and reagent consumption

2- Fluid volumes (µl; nl; pl; fl)

3- Small physical and economic footprint

4- Parallelization and high throughput experimentation

5- Unique physical phenomena [50] .

The microfluidic platform consists of a droplet generating device as and a micro-selector.

1-Droplet Generating Device. The chip has three fluid inlets that are linked to three micropumps through a T-junction to create droplets of various solutions. A steady force of micropumps moves the droplets. Each fluid was heated to the proper temperatures before being pumped into the microfluidic device.

2- Micro-selector. The micro-selector incorporates three uniquely modified channels. As the resistance force is different due to environment parameters, the velocity of each droplet is different. And due to the length of the channel each droplet pumped in, the time when they are pumped out is different from the

original order. Each channel has one droplet in it and another droplet can be pumped in only when the previous drop was pumped out. The process is parallelized by increasing the number of devices. In this way, the upper bound of time complexity is determined by the droplet which consumes the longest time for each device. When a droplet moves through the outlets of micr-oselector, It will be recognized by a sensor, which will then computer-record the sequence. A molecular code pad is produced once every droplet has exited the micro-selector. The used droplets can be gathered and ready for use again later [51].

Microfluidic Input Types

There are two types of microfluidic input fluids:

1- Newtonian Fluids : Because of the linear relationship between stress and strain, viscosity is independent of both stress and velocity.

2- Non-Newtonian Fluids : Non-linear relationship between shear stress and shear strain

Types of fluid flow:

1- Laminar : Fluid particles move along smooth paths in layers

2- Turbulent : An unsteady flow where fluid particles move along irregular paths [52].

2.5 Chaotic Theory

Chaos theory is a branch of mathematics that deals with nonlinear dynamical systems that have the butterfly effect [53] .

In recent years, chaos-based cryptosystem has gained immense attention in multimedia security. Due to the remarkable nonlinear chaotic properties, the

introduction of chaos in encryption has increased the strength of the cipher. The notable feature that makes it suitable for encryption is that it is sensitive to initial conditions even for a minute change in the initial parameters, a drastic change in the output is observed [54].

Because chaos and cryptography have certain subtle similarities, chaos was employed to create potentially efficient and secure cryptographic applications [55].

There are several conditions that must be met in order to observe chaotic behavior in a system. these conditions are listed below [56].

•The system must contain a nonlinear element.

•Continuous time systems should be at least third order. No such requirement is required for discrete-time systems. Even in a first order system, chaos can be observed.

•The behavior of the system should be extremely sensitive to the initial conditions and control parameters.

There are many types of chaotic map, that are well-known Logistic Map, Tent Map, Quadratic Map, Henon Map, Lorenz system, and others. This thesis concentrates on the logistic map [57].

Logistic Chaotic Maps: Is one of the most often used chaotic maps in chaotic cryptography since it is one of the most studied and widely utilized nonlinear systems. It is also used extensively in block ciphers, stream ciphers, and hash functions. A chaotic logical system is very sensitive to the initial conditions. The orbits of a logistic chaotic system may be split under the impact of mapping

regardless of how close the two points are since the points are extremely sensitive to the initial value [58]**.**

The expression of Logistic chaotic mapping is shown in Formula (2.1)

$$x_{n+1} = \mu x_n(1 - x_n),\ n = 0, 1, 2, 3 \ldots\ldots\ldots\ldots \quad (2.1) \quad [59]$$

2.6 Performance Metrics

There are many performance metrics have been used to test the performance of the proposed system such as:-

2.6.1 Execution Time

The time taken by the algorithm to perform the encryption and decryption of the input text files. The following are the parameters which calculate the performance of algorithm.

1- **Encryption Time**: It is the time that an encryption algorithm takes to produce a cipher text from a plain text. The encryption time is generally calculated in milliseconds Less encryption time, more will be performance of that algorithm.

2- **Decryption Time**: It is the time that an encryption algorithm takes to produce a plain text from a cipher text. The decryption time is generally calculated in milliseconds. Less is the decryption time, more will be performance of that algorithm.

2.6.2 Throughput:

The throughput of the encryption scheme is calculated as the total plain text in encrypted in Kbytes divided by the encryption time in milliseconds. The unit of throughput is MB/Sec. More is the throughput; more will be the performance. The throughput of the encryption scheme is calculated as the ratio of total plain text by

encryption time. The throughput of the encryption can be calculated as in equation (2.4).

$$\text{throughput} = \frac{\text{Tp(kilobytes)}}{Et(second)} \text{ ....……..(2.4)}$$

where Tp: size of plain text (Kilobytes).

Et: Encryption time (second) [60].

2.7 Security Metrics

Security metrics are used to assess the security level of a system and to implement security objective. It is important to establish a set of security metrics that measure the effectiveness of the system .

2.7.1 Randomness Tests

Randomness testing has a crucial and basic role in cryptography. Empirical tests of randomness are frequently used to assess randomness. Each test analyzes the data by focusing on a distinct attribute (number of ones, m-bit blocks, etc.). In order to give a more complex randomness analysis, tests are typically organized into test batteries, also known as test suites. The statistical test suites are of utmost relevance for evaluating any new source of (pseudo)randomness [61].

The NIST Test Suite is a statistical package consisting of 15 tests developed for the randomness testing of the binary sequences (word-for-word from the manual). Each test generates a P-value and a proportion value. Furthermore, a number sequence is assumed to be random when the P-value is more significant than 0.01, and the proportion value exceeds the minimum pass rate [62]. These 15 tests are listed in Table (2.2) [63].

Table (2.2) . List of NIST Statistical Tests [63]

Number	Test Name

1	Frequency
2	Block Frequency
3	Runs
4	Longest Run
5	Binary Matrix Rank
6	Discrete Fourier Transform
7	Non-overlapping Template Matching
8	Overlapping Template Matching
9	Universal
10	Linear Complexity
11	Serial
12	Approximate Entropy
13	Cumulative Sums
14	Random Excursions
15	Random Excursions Variant

Frequency Test

Through this test it is intended to see if the frequencies of 1 and 0 across the entire n-bit sequence are approximately equal that is the proportion of 1s and 0s is close to ½. 2. If the number of 0s and 1s are not same, it is intended to see if their difference falls within the limit of randomness.

Frequency Test within a Block

One can note that even if the first half on the n-bit sequence is full of 1 and the second half with 0, the test 1 would have passed although the sequence is highly non- random. Through this test it is intended to ensure that frequencies of 1 and 0 are evenly distributed across the entire n-bit sequence.

Runs Test

Runs of length k means exactly k identical bits bounded by bits of opposite value. In this test it is intended to see if the frequencies of runs of 1s and 0s of various lengths are in limits of randomness.

Longest Run of Ones in a Block

In this test it is intended to see if the frequencies of longest run of 1s appearing in the tested sequence are consistent with that expected for a random sequence. To execute the test the n-bit string is divided in N non- overlapping blocks each of M-bit such that N=[n/M]. The additional bits are neglected.

Binary Matrix Rank Test

Through this test it is intended to see if the n-bit string has repetitive patterns across its entire sequence. The n-bit string is sequentially divided into N disjoint blocks and it is endeavored to see linear dependence among its fixed length substrings of each block. Each block is represented by a matrix of M rows and Q columns such that N=[n/MQ]. The remaining unused bits are discarded. Usually both M and Q are taken as 32.

Discrete Fourier Transform Test

Through this test it is intended to see if the n-bit string has periodic features across its entire sequence. By periodic features one understands repetitive patterns that are close to each other.

Non-overlapping Template Test

By this test one intends to see template matching in a non-overlapping manner, i.e. it looks for occurrences of pre- specified non-periodic bit-string and to

see if the numbers of such occurrences are within the statistical limit of a sequence under the assumption of randomness.

Overlapping Template Test

Through this test one intends to detect template matching in an overlapping manner, that is, it looks for occurrences of pre-specified bit-string and to see if the number of such occurrences as against a sequence under the assumption of randomness.

Maurer's "Universal Statistical" Test

This test focuses to measure distances in terms of L-bit block-numbers between L-bit matching patterns. The distances are calculated using logarithmic function. The sum of log2 distances between L-bit matching patterns is necessary for statistic distribution. By this test one can conclude whether the sequence could be significantly compressed or not. A significantly compressible sequence is considered to be non-random.

Linear Complexity Test.

A long bit string is usually obtained from a LFSR (Linear Feedback Shift Register). The bit sequence from which a longer LFSR is obtained can be termed as random, while the shorter LFSR indicates non-randomness.

Serial Test

In long n-bit random sequence with at least one million bits, every m-bit pattern has the same chance of appearing as every other m-bit patterns. The

number of occurrences of the 2m m-bit overlapping patterns is approximately the same as would be expected of a random sequence.

Approximate Entropy Test

Entropy is a test of randomness based on repeating patterns. Larger is the entropy larger is the randomness. For n-bit string the entropy is measured by comparing the frequency of overlapping patterns of all possible m-bit patterns with that of (m+1)-bit patterns. The comparison between entropies of m and (m+1)-bit patterns is termed as approximate entropy, ApEn(m), which is compared against the expected result of a random sequence. For a random sequence, the ApEn(m) is a maximum value projected.

Cumulative Sums Test

This test looks whether 1s or 0s are occurring in large numbers at early stages or at later stages or 1s and 0s are intermixed evenly across the entire sequence.

Random Excursions Test

This test intends to look if the number of visits to a particular cumulative sums state within a cycle falls into a category that is expected of random sequence. Eight states, e.g. -4, -3, -2, -1 and +1, +2, +3, +4 are looked into – visits to states greater than +4 are clubbed within the visits to +4 state and visits to states lesser then -4 are clubbed within the visits to -4 state.

Random Excursions Variant

The Random Excursions Variant test looks for number of visits to a particular state in cumulative sums of random walk across the entire bit sequence and estimates deviations from expected number of visits in the random walk considering randomness [64].

2.7.2 Key Space

The key space is a set of all the potential keys that can be used in an encryption algorithm. An excellent encryption algorithm should have a large key space to resist the exhaustive attack [64]. In order to resist the brute force attacks, a cipher must have a sufficiently large key space. The minimum key size for symmetric ciphers are recommended to be at least 80 bits and 128 bits for lightweight and regular ciphers respectively [65].

Key length is equal to the number of bits in an encryption algorithm's key. A short key length means poor security. The key length determines the maximum number of combinations required to break an encryption algorithm, If a key is n bits long, then there are two to the nth power (2n) possible keys. For example, if the key is one bit long, and that one bit can either be a zero or a one, there are only two possible keys, 0 or 1. if the key length is 128 bits long, then there are 2128 possible keys [66].

2.7.3 Avalanche Effect

Avalanche effect is a desirable property of any encryption algorithm in which a small change in either the plaintext or the key should produce a significant change in the cipher text [67]. It is a measure of change in output. When input is changed by very few bits it causes significant change in output giving randomness. Randomness is a key requirement of encryption techniques, bits Avalanche effect

decides efficiency of encryption techniques. Avalanche effect can be calculated based on equation (2.2) [68] .

$$Avalanche = \frac{number\ of\ fliped\ bits}{\text{number of total}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.2)$$

If an algorithm fails to provide the avalanche effect to a required level, then a cryptanalyst can make predictions about the input data, being given the output. To estimate the degree of the avalanche effect in the transformation, an avalanche parameter was determined and used the numerical value of the deviation of the probability of a bit change in the output sequence in response to a bit change in the input sequence[69]. So a good cryptography algorithm should always satisfy the following equation:

$$\text{Avalanche} > 50\% \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.3)$$

This ensures that the attacker should not easily predict the cipher text from plain text or vice versa. The cryptography algorithm that does not satisfy the Avalanche effect equation and easily breached by the cryptanalyst [70].

2.8 Cryptanalysis

Cryptanalysis is a science that specializes in studying codebreaking methods for variety cryptosystems. The importance of Cryptanalysis of the various modern encryption systems is that it determines the level of security of cryptosystems [71].

2.8.1 Histogram

A histogram is a graph of the frequency distribution in which the vertical axis represents the count (frequency) and the horizontal axis represents the possible range of the data values [72] . For a good encryption, the distribution of cipher data of an encrypted data should be uniform or balanced**.**

The histogram shows how many times a symbol appears in some text , If the histogram of the cipher text has all symbols in a uniform way, the algorithm could resist a frequency attack [73]**.**

Histogram(X) creates a histogram plot of X. The histogram function uses an automatic binning algorithm that returns bins with a uniform width, chosen to cover the range of elements in X and reveal the underlying shape of the distribution. histogram displays the bins as rectangles such that the height of each rectangle indicates the number of elements in the bin [74].

2.8.2 Known Cipher Text Attack

In cryptography, a well-known cipher text attack is an attack model of cryptanalysis in which it is assumed that the attacker has access only to a set of cipher texts. it also has some knowledge of plain text. it has no idea what the secret key may be, The goal is to recover as much plaintext messages as possible or (preferably) to guess the secret key [75].

2.8.3 Brute Force Attack

A brute-force attack. uses trial-and-error to guess the cipher keys , it work through all possible combinations hoping to guess correctly.

The attacker relies on trying all possible keys. To avoid this type of attack, the number of possible keys must be very large [76].

The amount of time to breaking a cipher-text takes to implement is proportional to the size of key, which means that if the number of bits in the key is increased then the number of attempts will be increased, too [77].

Chapter Three

The Proposed Approach

3.1 Introduction

This chapter is intended to present the design of the proposed system. The basic principle of the proposed system is to use the nonlinearity behavior in generating the cipher key, where the first level of randomness is the use of microfluidic technology to generate a set of keys (key pad) from which the seed key is chosen. The second level is represented by the use of chaotic system (logistic map) in order to adapt the key length to the message length to obtain a strong, secure and unbreakable guessable cipher key to be used in the encryption process. The encryption algorithm is a symmetric stream code uses DNA coding with XOR operation to obtain a cipher text in DNA format.

The outline of this chapter presents as a block diagrams, flow charts, figures and algorithms with explanation the main stages, their input and output.

3.2 The Design of the Proposed System

The proposed system consists of sender site and receiver site. The sender site includes three main parts (key pad generation, seed key selection, key expansion, encryption process). On the other hand, the receiver site contains the inverse phases of the sender site. As shown in figure (3.1)

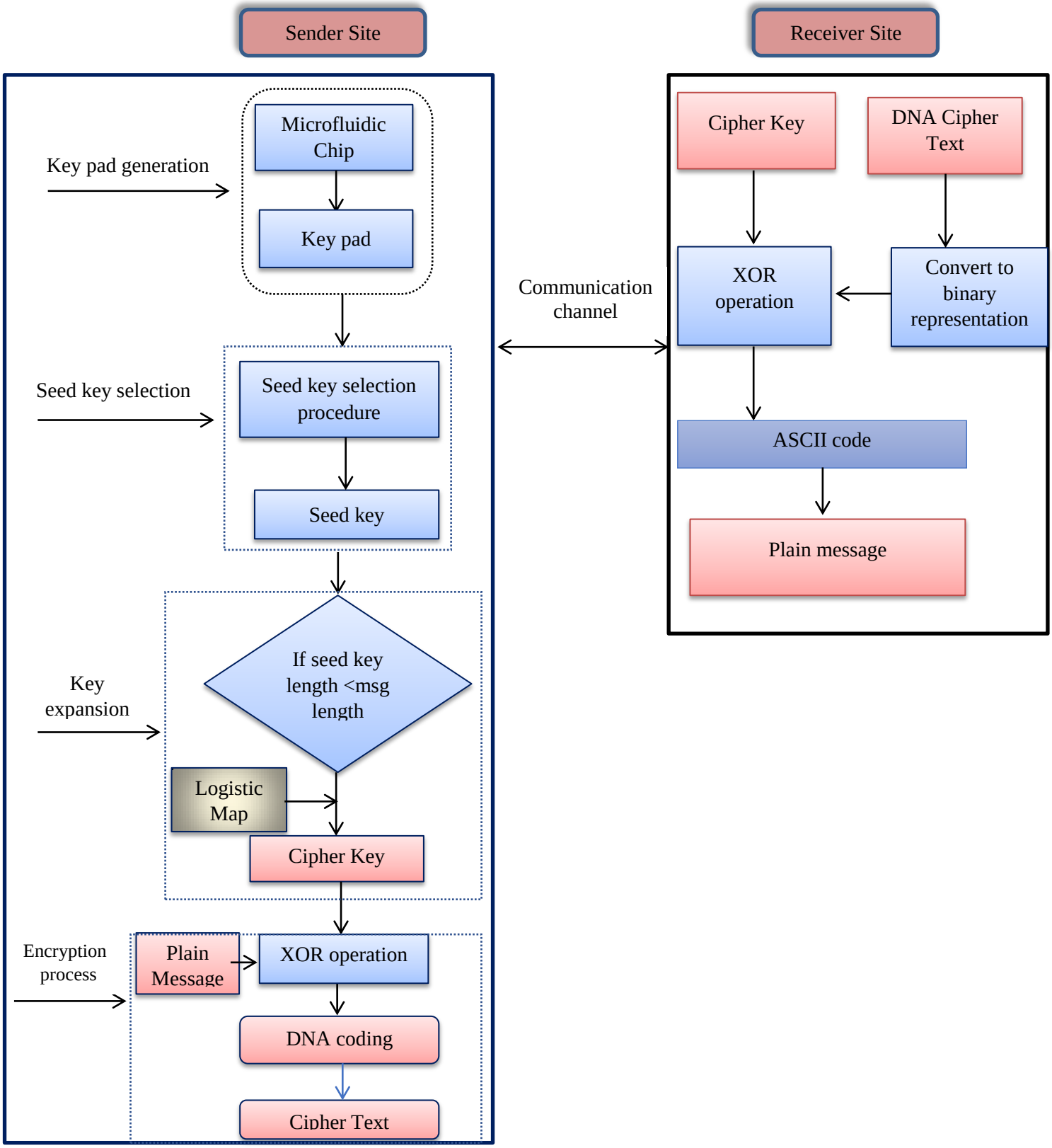


Figure (3.1) : Proposed System Block Diagram

3.2.1 Sender Site Activities

The sender applies number of activities on the message before send it to the receiver through a communication channel. Each activity has its own processes. The output of these activities are integrated with each other to construct a multilayers of security.

3.2.1.1 Key Pad Generation

The key pad generation process based on the nonlinearity flowing random strings using in the microfluidic chip. The format of this pad is a DNA sequence.

The nonlinearity behavior is simulated by (n) random strings with three inlet channels, a mixer is used to mix the input of these channels as an input to the selector. Where the selector stage has two channels :-

The first channel is the accepted character form while the second channel represent the reject character (Drop). Figure (3.2) and algorithm (3.1) clarify key generation procedure.

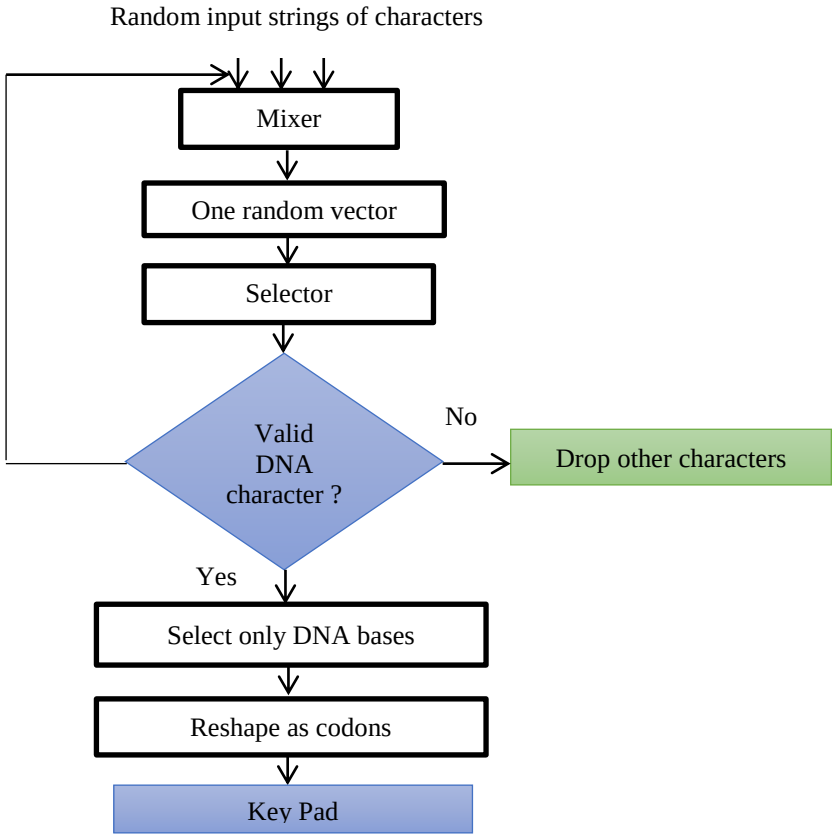


Figure (3.2): Key Pad Generation Procedure

Algorithm (3.1): Key Pad Generation

Input (n random strings of characters).

Output (pad of DNA keys).

Begin

Step 1: Determine the required matrix dimensions (key pad dimensions)

Step 2: Generate 3 random strings of characters (input to microfluidic).

Step 3: Mix strings from previous step (mixer in microfluidic)

Step 4: select only four bases of DNA(A,C,G,T) (selector in microfluidic)

Step 5: Drop other characters

Step 5: Reshape the four DNA bases from (step 4) as codons (Triple bases)

Step 6: Put codons from previous step in a matrix whose dimensions are determine in (step 1)

End

3.2.1.2 Seed Key Selection Procedure

To select a proper seed cipher key from the generated key pad, several process done such as highest weight, least recursion. The procedure of these processes illustrated in figure (3.3) and algorithm (3.2).

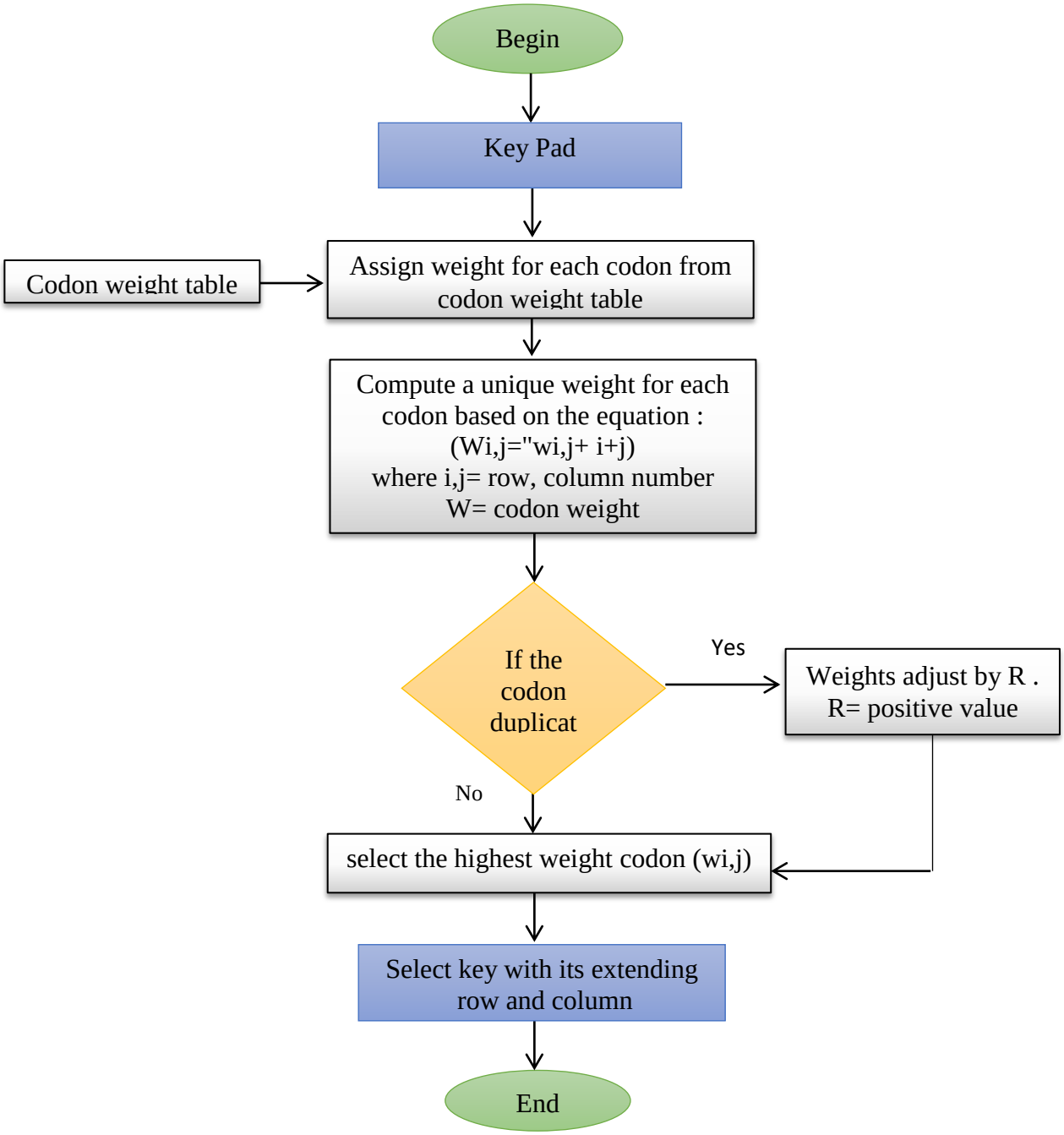


Figure (3.3): Seed Key Selection Procedure

Algorithm (3.2): Seed Key Selection

Input (Key Pad (**S** ,Codons Table (**C**), Codon Weights Table (**W**))

Output (Seed Key)

Begin

Step 1: Each codon is assigned to weight in the key pad based on codon weights tables .

$$S(i,j) = W(c(i,j))$$

Step 2: To compute unique weight for each codon apply the following equation.

$$W_{i,j} = W_{i,j} + i + j \quad \text{..... (.3.1)}$$

(where: i,j are row and column numbers)

Step 3: If the codon is repeated more than once, then adjust the weight of the duplicate codon according to the following equation

$$W_{i,j} = W_{i,j} - R \text{.....(3.2)}$$

$$R = R + X \text{.....(3.3)}$$

where **R,X** = positive value

step 4: Find the highest codon weight with its extension to be the key

step 5 :The result is the best selection seed key

End

3.2.1.3 Encryption Process

The encryption procedure stated to encrypt the message using the selected seed key to produce a ciphered message in DNA format. This process composed of two parts, as shown in the algorithm (3.3).

Before the encryption process takes a place a checking step is used for knowing the length of the (message and seed key), if they are same or not. In case of not,

a manipulation is done to the key length to be equalized with the message length according to the steps below :

1. If the message length is less than seed key length then cuts a part of seed key equal to message length
2. If the message length is greater than seed key length then uses chaotic map (logistic map) to generate random binary numbers equal to the difference between message length and seed key length after that combine it with the binary representation of seed key to produce cipher key.

apply the XOR operation between message and cipher key (binary representation) getting a binary array.

The resulted array converted to DNA bases (A,C,G,T) to get cipher message . which is sent to the receiver.

The encryption process in algorithm (3.3), figure (3.4).

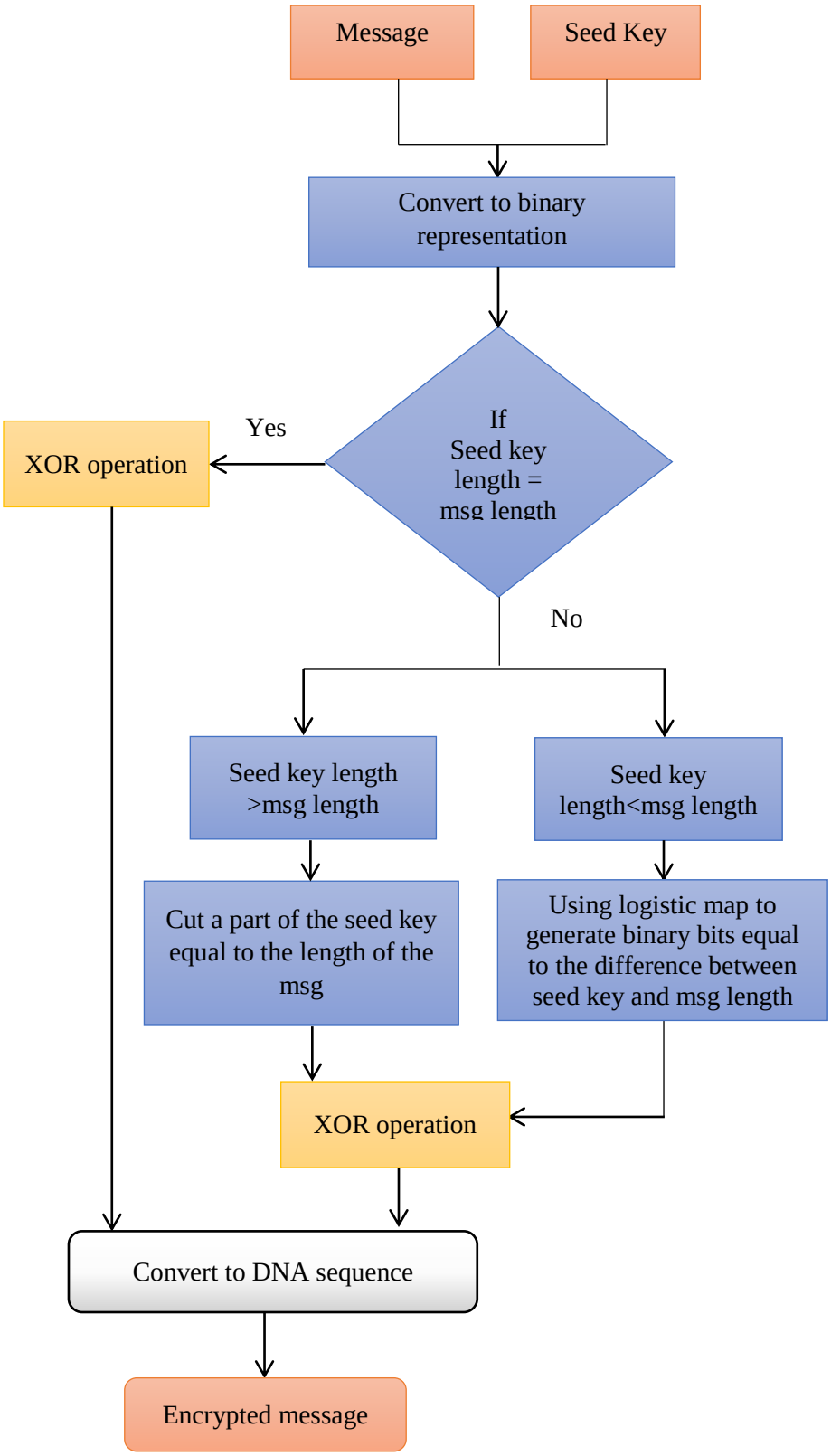


Figure (3.4) : Encryption Process

Algorithm (3.3) Encryption Process

Input = Text message, Seed Key

Output = Cipher Text in DNA Format

Begin

Step 1: Convert the message and seed key to binary representation

Step 2: compute the length of message and seed key

Step 3: compare the length of message and seed key to get the cipher keys. According to the following: -

- If message length is equal to seed key length, then go to (step 4)
- If message length is less than seed key length then Cuts a part of the seed key equal to the length of the message and go to (step 4).
- If message length is greater than seed key length then Use logistic map to generate binary numbers equal to the difference between the length of the seed key and the message, then combine it with the seed key to obtain the cipher key.

Step 4: Apply XOR operation between binary message and cipher key

Step 5: Convert the vector resulted from previous step to DNA sequence based on (Rule 1) in (Table 2.1) to get the cipher text

End

3.2.2 Receiver Site Activities

In receiver site, after receiving the encryption message. The receiver decryption the cipher message to retrieve the original message by reversing the sender processes .

- Decryption Process

The encrypted message reaches at the receiver side which is in the form of DNA sequence. The receiver receive a copy of secret key from a secured channel upon a previous agreement protocol transfer between the sender and receiver which must be used only once and being destroyed, so The decryption process is done by reversing the encryption steps to get the plain message, as shown in figure (3.5) and algorithm (3.4):-

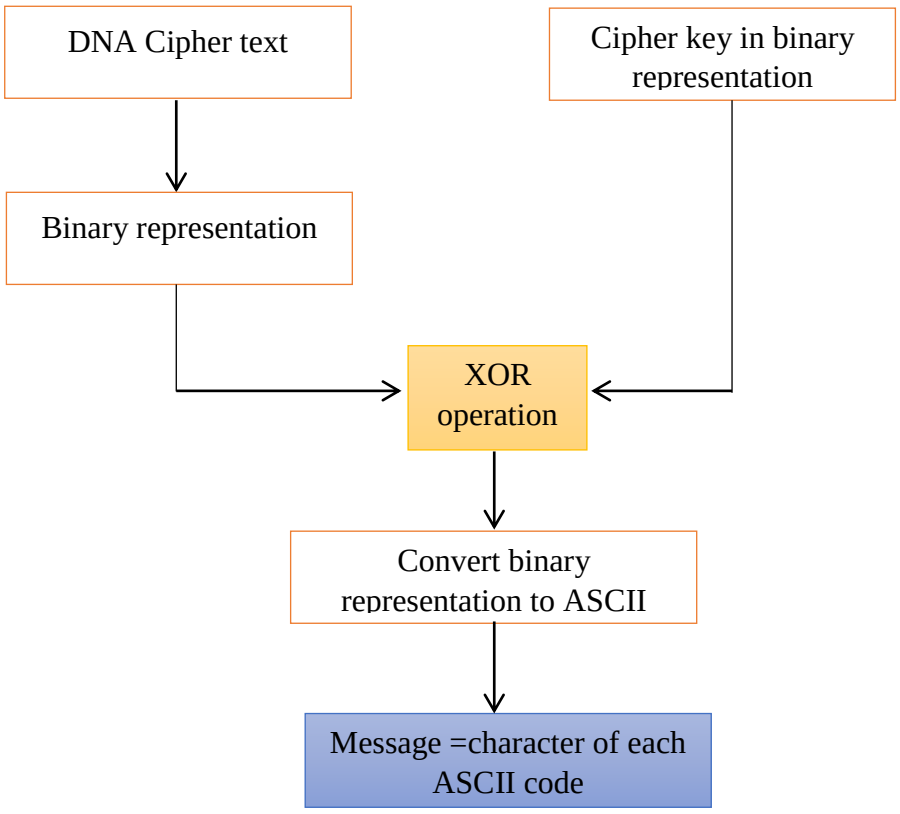


Figure (3.5) Decryption Process

Algorithm (3.4) Decryption Process

Input : Cipher Message , Cipher Key .

Output : Original Message (Plain-Text) .

Begin

Step 1: Convert cipher text to binary representation

Step 2: Apply XOR operation between cipher key and binary cipher text

Step 3: Convert binary vector resulted from previous step to ASCII code

Step 4: Convert ACII code to the corresponding character to get the original message

End

3.3 Summary

The proposed algorithm consists of several stages represented by (generate a set of keys (key pad) using microfluidic technique, select seed key based on codons and its weight with proposed equations, seed key expansion by using logistic map, encryption process based on DNA coding and XOR operation) in order to provide multiple layers of encryption to obtained cipher text at last becomes more secure than conventional DNA techniques because the resulting cipher text comes in the form of unreadable, unpredictable, ambiguous text that creates confusion during the decryption process.

Chapter Four
Results and Performance Evaluation

4.1 Introduction

This chapter describes the experimental results carried out to evaluate the performance of the proposed scheme. In addition, it introduces a discussion of the experimental work results for evaluating the performance of the system. We use messages with various sizes to test the proposed scheme, the estimated storage size in Kilobytes.

The proposed algorithm techniques have been implemented (using MATLAB program version R2022a on Windows 10 platform on Intel core i5). The experimental results were analyzed to clarify the results by some performance metrics that are discussed in chapter two.

4.2 Methodology

The proposed methodology implementation pass through the following stages :-

4.2.1 Key Pad Generation Stage

The first part of the proposed system is to generate a random key pad (set of keys) according to the following steps :-

1- Determining the dimension of key pad matrix . For example (5*5)

2- Generating three random strings of characters according to the used channels.

- {'RzgzrqPJBo5a5tP0jh6tr:kthj…'}
- {'VA59GYt1jHCOgVzW7jhggTf321cb…'}
- {'OVXzqcFTRsICqtcR7G5bvAEqA2<;'fd…'}

Mixing Step

'RzgzrqPJBo5a5tP0jh6tr:kthjVA59GYt1jHCOgVzW7jhggTf321cbOVXzqcFTRsI CqtcR7G5bvAEqA2<;'fd……}

3- Selector Step, has two direction :-

Direction 1: the required characters is the four DNA bases (A,C,G,T), the selector select only these bases from the previous step and saved in a vector (X) .

Selector ={GATTAGTCGGGTCCTCTCGAA……}

Direction 2: dropping the miss matching characters that not match with the four bases

Drop={'q;IL*Zvd2BzJ7BOwjqzsoQ1n8XJ;Lo55uv4d0swy1W6SpPf;Oz5O4H9BX k280YBVLNxVkLKKU;,……}

4- Reconfiguring Step: reconfigure the vector (X) as a codon matrix with dimension (for example 5*5) as shown in figure (4.1)

AAT	**GAA**	**GTA**	**TAT**	**GTG**
GTA	**GGT**	**CCG**	**GGT**	**AGG**
GAA	**TCG**	**AAT**	**TCT**	**ACG**
CCT	**ATG**	**TTT**	**CAC**	**TCA**
TCC	**GGT**	**ATG**	**AAG**	**AGG**

Figure (4.1): Key Pad (Codon Matrix of (5*5))

4.2.2 Stages of Seed Key Selection

The second part of the proposed system is the selection of seed key. where the inputs for this part are :-

- Key pad (figure 4.1).

- Codon Table (Table (4.1)).
- Weight codon Table (Table (4.2)).

Table (4.1): Codon Table

AAA	AAC	AAG	AAT	ACA	ACC	ACG	ACT
AGA	AGC	AGG	AGT	ATA	ATC	ATG	ATT
CAA	CAC	CAG	CAT	CCA	CCC	CCG	CCT
CGA	CGC	CGG	CGT	CTA	CTC	CTG	CTT
GAA	GAC	GAG	GAT	GCA	GCC	GCG	GCT
GGA	GGC	GGG	GGT	GTA	GTC	GTG	GTT
TAA	TAC	TAG	TAT	TCA	TCC	TCG	TCT
TGA	TGC	TGG	TGT	TTA	TTC	TTG	TTT

Codon table used to translate a genetic code into a sequence of amino acids (A, U, G, C). There are 64 different combinations of codon in codon table.

Table (4.2): Weight Codon Table

128.17	114.11	128.17	114.11	101.11	101.11	101.11	101.11
156.19	087.08	156.19	087.08	113.16	113.16	131.19	133.16
128.14	129.10	128.14	137.14	097.12	097.12	097.12	113.16
156.19	137.14	067.12	156.19	113.16	113.16	113.16	113.16
129.12	115.09	129.12	115.09	071.90	071.90	071.90	071.90
103.15	071.90	103.15	103.15	099.14	099.14	099.14	099.14
128.12	163.18	163.15	163.18	087.08	087.08	087.08	087.08
186.18	103.15	186.21	103.15	113.16	147.18	113.16	147.18

For each codon in the table (4.1) there is a corresponding weight in the table (4.2). There are more than one codon that has the same weight.

- The process of selecting the seed key pass through:-

1- Depending on generated key pad (figure (4.2)) , a weight is assigned for each codon, based on the weights table as shown in figure (4.3)

TTG	GTA	ACC	TCT	TTC
GAC	GTA	ACA	AGC	TCC
TTC	CTT	CCA	TTT	CTG
TCC	TCG	AGC	AGT	TAA
ATA	CGA	TGC	CGT	GCT

Figure (4.2): Key Pad (5*5)

113.16	99.14	101.11	87.08	147.18
115.09	99.14	101.11	87.08	87.08
147.18	113.16	97.12	147.18	113.16
87.08	87.08	87.08	87.08	128.12
113.16	156.19	103.15	156.19	71.9

Figure (4.3): Key Pad Assign Codons Weight

Each number in figure (4.3) represents the weight corresponding to each codon in figure (4.2) based on table (4.2).

2 - Calculating a unique weight for each codon as shown in figure (4.4)

115.16	102.14	105.11	92.08	153.18
118.09	103.14	106.11	93.08	94.08
151.18	118.16	103.12	154.18	121.16
92.16	93.08	94.08	95.08	137.12
119.16	163.19	111.15	165.19	81.9

Figure (4.4): Unique Weight for Each Codon

In figure(4.4) the problem of repeated weights has been solved, as each codon in figure(4.2) has a unique weight based on eq. (3.1).

3- Find the repeats codon and adjust its weight depending on eq. (3.2) , (3.3) .As shown in figure (4.5).

115.16	102.14	105.11	92.08	153.18
118.09	103.14	106.11	93.08	94.08
141.18	118.16	103.12	154.18	121.16
82.08	93.08	84.08	95.08	137.12
119.16	163.19	111.15	165.19	81.90

Figure (4.5): Adjusted Weights

In figure (4.5) the unique weights remain the same as in figure (4.4), but the repeated weights decrease each time by the value of (R), (R=10).

4- To find the seed key, take the codon of highest weight with its related row and column where its located .

Seed key = "CGTATACGATGCGCTTCTAGCTTTAGT"

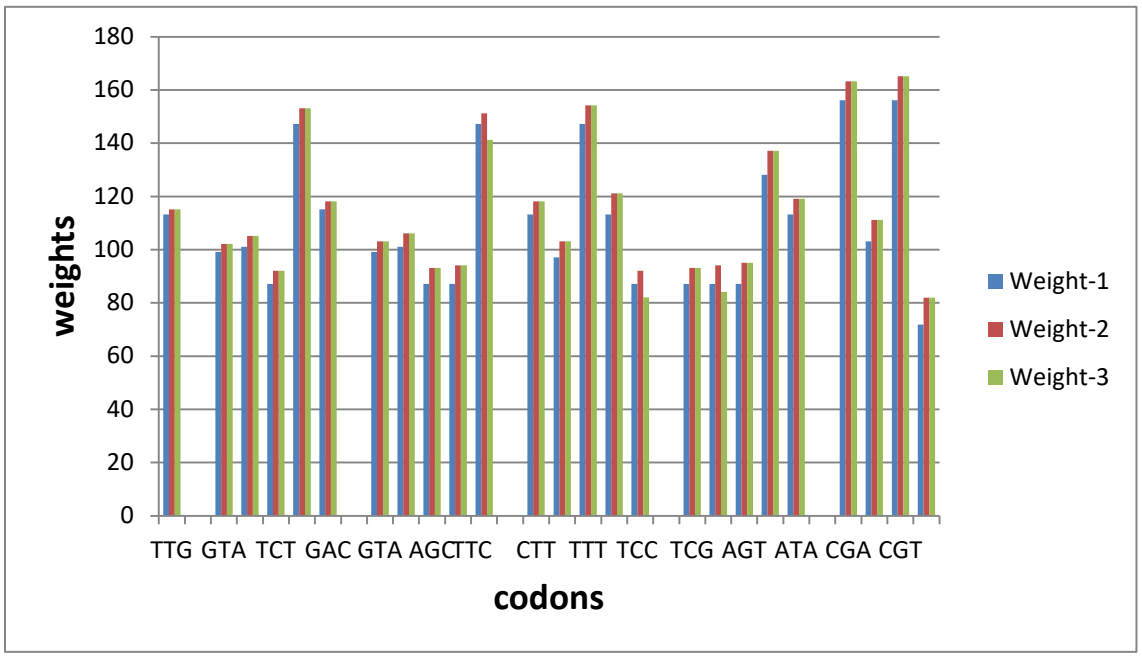


Figure (4.6): Weights Adjustment Diagram

Figure (4.6) represents the stages of adjusting the weights to obtain the final seed key .

4.2.3 Encryption Procedure Stage

The encryption process consists of several stages as shown below :-

Step1 – converting seed key and message to binary form**.**

Step 2: equalizing of the seed key length with the length of the message using the logistic map to generate random binary numbers that are combined with the binary numbers of the seed key.

Seed key = CGTATACGATGCGCTTCTAGCTTTAGT

Message = "DNA cryptography represents a new field in cryptology", as shown in results bellow:-

❖ Converting seed key and message to binary representation as shown below:

Key Binary Representation

1101011110111100101110001101100001100111100100110000100110100101101
1011010101110110000000000000000000000000000010100001000011010001110
0010000000000000000000000000011111111111111111111111111

Length of seed key is **189 bit**

Message Binary Representation:

0010101001101001001001110010100110011000100101001011101001100011110
0000100101010100010101000000101100010110110000000111000000000100101111
0000111010111001000000111110010000100100001100000000010000001000010101
0110001001110100000011110010101010110100110000010000000000000011110000
1000111111111111111111111111111111111111111111111111111111111111011111111
1111011111111111010111011111011011111111111

Length of message is **371 bit**

❖ generate a number of random bits equal to the difference between the key length and the message length to get the cipher key

the difference is: **371-189 = 182**

according to the difference value there is a need to generate (182) random binary bits. This is done using logistic map.

Therefore, the cipher key will be:

1101011110111100101110001101100001100111100100110000100110100101101
1011010101110110000000000000000000000000000010100001000011010001110
0010000000000000000000000000011111111111111111111111111110110000
0001011000011100001100011110000011000111100011110101001000000110101
0010000001110000110001111000111100011110001111100001110000110101001
00011110000001100000111000011000111100011.

Step 3 : Apply XOR operation between the message and cipher key bits.

1111110111010101100111111111000111111111000001111011001111000110001011110000100010010101000000101100010110110010101111000011110100000010111010111001000001111100101110111011110011111111011111010111010011101000011010000010111111011010110101110000011010101001000110001011010111100011110011100001110000111000011100000111100011111010101101110100111110010101001111101110000111000.

Step 4: converting the result of step (3) to a DNA bases based on rule (1) of table (2.1) to obtain the cipher message.

Cipher message:-

TTTCTCCCGCTTTTACTTTTAACTGTATTACGAGTTAAGAGCCCAAAGTACCGTAGGTTAATTCAAAGTGGTGCAACTTAGTGTCTGCTTTGTTGGTGGCTCACGGAAGTTGTCCGGTGAATCCCAGATACCGGTTACTGCTAATGACTAATGAATTACTTCCCGTGGCTTAGGGCTTCTAACTA

4.2.4 Decryption Process Stage

The decryption process is done by reversing the encryption steps to get the plain message, as shown in the following steps :-

Step 1: Converting DNA sequence into binary representation based on rule(1) of table(2.1).

Cipher Text:-

TTTCTCCCGCTTTTACTTTTAACTGTATTACGAGTTAAGAGCCCAAAGTACCGTAGGTTAATTCAAAGTGGTGCAACTTAGTGTCTGCTTTGTTGGTGGCTCACGGAAGTTGTCCGGTGAATCCCAGATACCGGTTACTGCTAATGACTAATGAATTACTTCCCGTGGCTTAGGGCTTCTAACTA

DNA Binary coding: -

1111110111010101100111111111000111111111000001111011001111000110001011110000100010010101000000101100010110110010101111000011110100000010111010111001000001111100101110110111100111111111011111010111010111010000011010000010111111011010110101110000011010101001000110001011010111100011110011100001110000111000011100000111100011111010101101110100111111001010100111110111000001110

Step 2: Apply XOR operation between cipher key and DNA binary coding :

00101010011010 0100100111001010011001100010010100101110100110001110000010010101000101010000001011000101101100000011100000001001011100000111001000001111100100000100100001100000000100000100001010011000100111010000011110010101010110100110000010000000000001111000010000111111111111111111111111111111111111111111111111111111111011111111111101111111110101110111110110111111111111

Step 3: Converting binary vector resulted from previous step into ASCII code:

68	78	65	32	99	114	121	112	116	111	103	114
97	112	104	121	32	114	101	112	114	101	115	101
110	116	115	32	97	32	110	101	119	32	102	105
101	108	100	32	105	110	32	99	114	121	112	116
111	108	111	103	121							

Step 4: Converting the ASCII code into its corresponding symbols, to get the original message

Message = " DNA cryptography represents a new field in cryptology "

4.3 Experimental Results and Analysis

To clarify the performance of the proposed system, several measuring metrics are used such as:

4.3.1 Security Test Results

4.3.1.1 Randomness Test of the Ciphered Key

This section discusses the randomness tests performed on the seed key in order to assess the security of the proposed system. The measuring randomness test used is the NIST test suite.

The significance level (α) of the test of a statistical hypothesis for the tests is selected to be 0.01. If $p \geq \alpha = 0.01$ then with confidence level 99%, we can say that the generated key stream is random and if $p < \alpha = 0.01$ then the key stream is said to be non-random with confidence level of 99%. The used tests are

Table (4.3): Seed Keys Randomness Test

Pad	Frequency Test	Frequency Test within a block	Long Runs of Ones Test
3*3	0.2830	0.5120	0.00012
4*4	0.3642	0.008	0.0330
5*5	0.0689	0.0518	0.1870
7*7	0.0606	0.0001	0.0003
9*9	0.0495	0.0003	0.0041
11*11	0.0014	0.00041	0.0003
15*15	0.0038	0.00007	0.00003

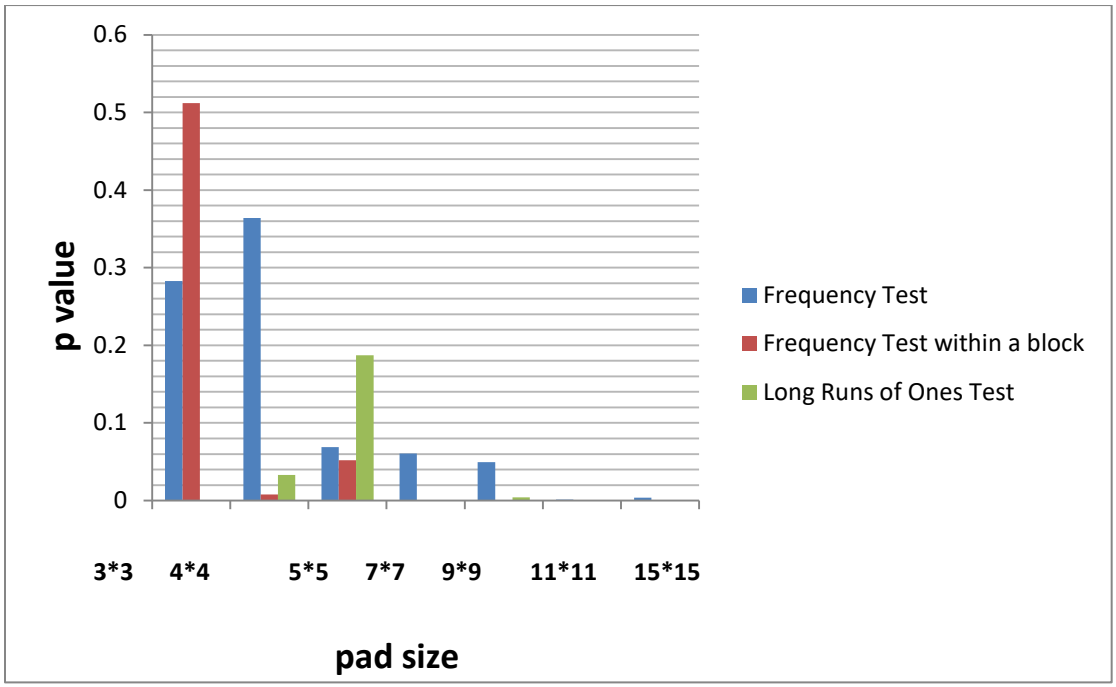


Figure (4.7): Seed Key Test .

From figure (4.7) it is noted that as the length of the seed key increases, the percentage of randomness decreases. The reason is because the seed key consists of only four character (A,C,G,T). To solve this problem, logistic map issued logistics map to obtain longer keys with good random percentages. It is clear that the (3*3) key pad achieved the highest random proportions compared to the other dimensions . It should be noted that every time we generate a seed key from different key pad dimensions get different random percentages.

4.3.1.2 Avalanche Effect.

To show any slight change in either the key or the plain-text that result in a significant change in the cipher-text. As shown table (4.4).

Table (4.4): Avalanche Effect

File size	Avalanche Effect
1 KB	78.39 %
2 KB	65.13 %
3 KB	78.28 %

The higher the avalanche effect is the better the security will be. The given scenario where the attacker has access to cipher text tries to establish a relationship between cipher text and its plaintext. If changing one bit results in a change of more than 50% bits, it becomes challenging for the attacker to retrieve the original message as (1KB,3KB) while (2KB) has lower security.

4.3.1.3 Key Space Analysis

The total number of key space depends on the dimensions of generated key pad. By using (5*5) key pad the key length = 200 bit that making seed key space (2^{200}). Then in the second stage, the length of the key is increased by using the map to match the length of the message, which makes the key achieve randomness in two stages, the generation stage and the stage of adaptation with the message.

The key of the proposed algorithm is secure enough to resist all kinds of brute-force attacks and can provide a high security level.

4.3.2 Performance Results

4.3.2.1 Encryption and Decryption Time :

- **Encryption Time**

It is the time that an encryption algorithm takes to produce a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption process. In other words, it indicates the speed of the encryption process. The encryption time is generally calculated in milliseconds. It is the time taken by an encryption algorithm to encrypt the data. Less is the encryption time; more will be performance of that algorithm.

- **Decryption Time:**

It is the time that an encryption algorithm takes to produce a plain text from a cipher text. Decryption time is used to calculate the throughput of a decryption process. In other words, it indicates the speed of the decryption process. It is the time taken by an encryption algorithm to decrypt the data.

Table (4.5): Encryption and Decryption Time (in millisecond)

File size	Encryption time	Decryption time
1 KB	0.104397	0.103321
2 KB	0.2078	0.205619
3 KB	0.302262	0.307721

4.3.2.2 Encrypted File Size

In cryptography, the term expansion of the cipher text refers to the increase the length of a plain text when it is encrypted. Many modern cipher systems cause a certain degree of expansion during the encryption process. Probabilistic cipher schemes cause expansion of the cipher text, where the set of possible cipher texts is necessarily larger than the set of explicit texts for the input. Table (4.6) represents size of .txt files before and after encryption.

Table (4.6): plain and cipher text files of different sizes

plain text file	Cipher text file
1KB	3.36 KB
2KB	6.69 KB
3KB	9.84 KB

4.3.2.3 Throughput

The throughput of the encryption scheme is calculated as the total plain text in encrypted in Kbytes divided by the encryption time in milliseconds. The unit of throughput is MB/Sec.

Algorithms that has minimum encryption time and maximum throughput due to its better performance.

Table (4.7): Throughput of different file size

Plain text file	Throughput
1 KB	9.1046
2 KB	8.8899
3 KB	6.9351

4.3.2.4 Bit Error Rate (BER)

The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. Bit error ratio is a unit less performance measure, often expressed as a percentage. Table (4.8) shows the BER of different messages length.

Table (4.8): Bit Error Rate

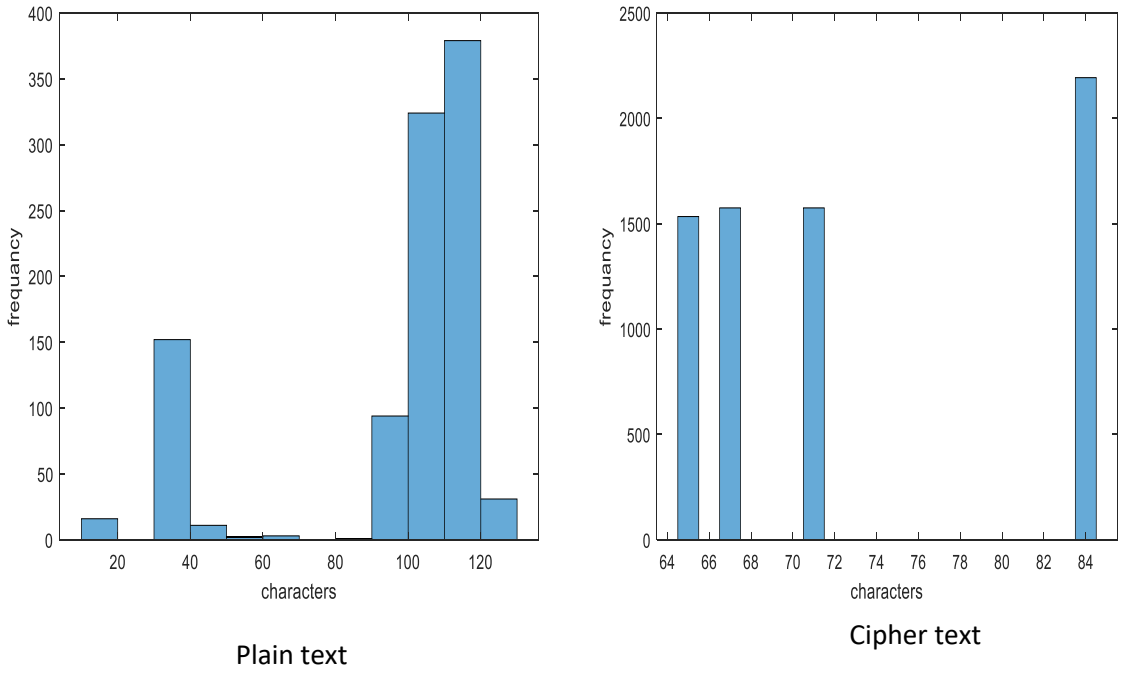
Length of message in byte	**BER**
1KB	0.2086
2 KB	0.4011
3 KB	0.5597

4.4 Cryptanalysis

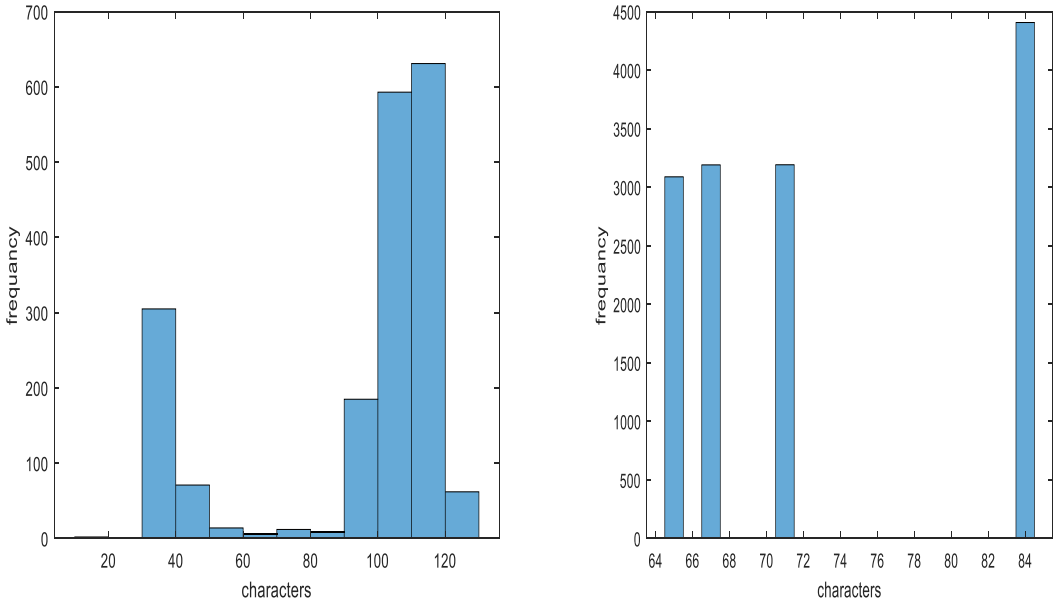
To analyze the proposed system ciphering process performance, the flowing metrics and attacks are used:

4.4.1 Histogram Analysis

The text histogram illustrates that how the characters in the text file are distributed by plotting the frequency of the characters .The distribution of cipher-text is of much importance. More specifically, it should hide the redundancy of plaintext and should not leak any information about the plain-text or the relationship between plain-text and cipher-text. The analysis of the histograms of three files (1KB,2KB,3KB) as a plain-text and its ciphered text are shown in figures (4.10), (4.11) and (4.12). It's clear that the histograms of the cipher-text are fairly uniform and significantly different from that of the plain text and hence do not provide any clue to employ statistical attack.

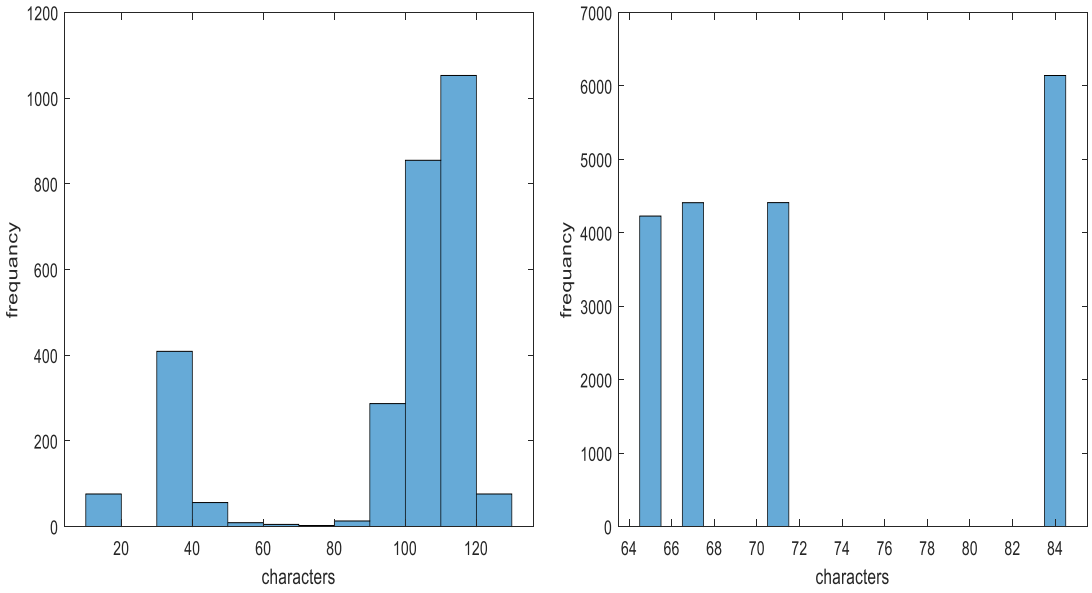


Figure(4.8): Histogram of 1KB File Size



Plain text Cipher text

Figure(4.9): Histogram of 2KB File Text Size



Plain text Cipher text

Figure(4.10): Histogram of 3KB File Text Size

4.4.2 Known Cipher Text Attack

In cryptography, a well-known cipher text attack is an attack model of cryptanalysis in which it is assumed that the attacker has access only to a set of cipher texts. He also has some knowledge of plain text. He has no idea what the secret key may be ,The goal is to recover as much plaintext messages as possible or (preferably) to guess the secret key.

To resist this kind of attack, the algorithm's resistance to decrypting the text must be very high , and this depends mainly on the strength of the key and its resistance . This is the goal of our proposed method by making the process of obtaining the cipher key not depend on traditional encryption methods or mathematical equations that can be guessed or broken, it has been adopted hybrid methods and proposed equations for method to get an unbreakable cipher text.

4.4.3 Brute Force Attack

A brute-force attack. uses trial-and-error to guess the cipher keys , he work through all possible combinations hoping to guess correctly.

In this method, the attacker relies on trying all possible keys .To avoid this type of attack, the number of possible keys must be very large .and this is the working principle of proposed method, as the number of attempts to obtain the cipher key requires a huge number of guesses, and even if the attacker succeeds in guessing one of the stages of obtaining the cipher key, he still has many stages to guess, as shown in the following steps:-

- Guessing the number of entries in the microfluidic stage.
- Guessing the selection condition in the selector procedure.
- Know that each element of the codon matrix is three letters of DNA bases (codon)
- Obtaining the codon table.
- Obtaining the weights table.
- Guessing the dimensions of the codon matrix and its corresponding weights.
- Guessing the equation for assigning a unique weight to each codon.
- Guessing the equation for decreasing the importance of the repeating codon and obtaining the codon with the highest weight.
- Guessing the procedure for obtaining the seed key from the intersection of the row and column at the codon with the highest weight.
- Even if the attacker guesses all the previous stages successfully and gets the seed key, he still has another challenge, which is to get the cipher key. Which includes a number of sub-steps as shown below :-
- Calculating the difference between the seed key length and the message length.
- Generating random bits using logistic map equal to the difference between the length of the message and the length of the seed key
- Combining the generated bits with the seed key bits.

As a result, the brute force attack has a huge number of attempts, and this makes it very difficult to obtain the correct cipher key

4.5 Comparison

In this section, the performance of our presented algorithm is compared with Ref [15], [16] under (avalanche effect, encryption and decryption time).

Table (4.9) Comparison of the Proposed System with Ref(15,16)

File size	Ref	Encryption time	Decryption time	Avalanche
1KB	[15]	2.578	2.625	———
	[16]	———	———	70 %
	proposed	0.104397	0.103321	78.39 %
2KB	[15]	3.406	3.734	———
	[16]	———	———	73 %
	Proposed	0.2078	0.205619	65.13 %
3KB	[15]	12.515	12.203	———
	[16]	———	———	82 %
	proposed	0.302262	0.307721	78.28 %

Chapter Five
Conclusions and future Works

5.1 Introduction

This chapter presents the conclusions educed from the proposed work with several suggestions for a future work.

5.2 Conclusions

The current research has come up with the following conclusions, based on the implemented results.

1- Using the logistic map for extend the seed key has a benefit in get a new cipher text to the same plain message and cipher key.

2- Microfluidic technique gave new methods of input characterized by flexibility and a high level of randomness

3- In the proposed system logistic map system is used, because this system has the characteristics of high security and efficiency. Increase the complexity and unpredictability of the proposed system.

4- DNA binary strands support feasibility and applicability of DNA-based Cryptography. The security and the performance of the DNA based cryptographic algorithms are satisfactory for multilevel security applications of today's network.

5.3 Future Works

Several suggestions are adopted here to extend the current proposal as a future work in this thesis:

1- Using DNA operations like (subtraction, addition) to adapt the key length to the message length

2- Using of RNA computing in the proposed algorithm to encrypt message.

3- Apply the proposed algorithm with image, audio and video.

References

[1] Ibrahim, D., Ahmed, K., Abdallah, M., & Ali, A. A. (2022). A New Chaotic-Based RGB Image Encryption Technique Using a Nonlinear Rotational 16× 16 DNA Playfair Matrix. Cryptography, 6(2), 28.

[2] Kolate, V., & Joshi, R. B. (2021). An information security using DNA cryptography along with AES algorithm. Turkish Journal of Computer and Mathematics Education, 12(1S), 183-192.

[3] Abd El-Latif, A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., Elwahsh, H., Piran, M. J., Bashir, A. K., ... & Mazurczyk, W. (2020). Providing end-to-end security using quantum walks in IoT networks. IEEE Access, 8, 92687-92696.

[4] Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.

[5] Rai, S., Choubey, V., & Garg, P. (2022, July). A Systematic Review of Encryption and Keylogging for Computer System Security. In 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT) (pp. 157-163). IEEE.

[6] Martin, K. (2020). Cryptography: The key to digital security, how it works, and why it matters. WW norton & Company.

[7] Reddy, M. I., Kumar, A. S., & Reddy, K. S. (2020). A secured cryptographic system based on DNA and a hybrid key generation approach. Biosystems, 197, 104207

[8] Kumar, B. M., Sri, B. R. S., Katamaraju, G. M. S. A., Rani, P., Harinadh, N., & Saibabu, C. (2020, March). File encryption and decryption using DNA technology. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 382-385). IEEE.

[9] Gupta, L. M., Garg, H., & Samad, A. (2019). An improved DNA based security model using reduced cipher text technique. International Journal of Computer Network and Information Security, 11(7), 13-20.

[10] Manucom, E. M. M., Gerardo, B. D., & Medina, R. P. (2019, October). Analysis of key randomness in improved one-time pad cryptography. In 2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID) (pp. 11-16). IEEE.

[11] Hazra, A., Ghosh, S., & Jash, S. (2018). A new DNA cryptography based algorithm involving the fusion of symmetric-key techniques. In Advanced Computational and Communication Paradigms (pp. 605-615). Springer, Singapore.

[12] Nath, A., & Dodia, A. (2018). Symmetric Key Encryption Algorithm using DNA Sequence. International Journal, 6(4).

[13] Zheng, J., & Liu, L. (2020). Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. IET Image Processing, 14(11), 2310-2320.

[14] Ragavan, M., & Prabu, K. (2019). Dynamic key generation for cryptographic process using genetic algorithm. International Journal of Computer Science and Information Security (IJCSIS), 17(4), 246-250.

[15] Thanikaiselvan, V., Routhu, B. K., & Sasank, J. V. (2019, March). Index Based Multiple Image Cryptosystem Using DNA Sequence. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-6). IEEE.

[16] Tahat, N., Tahat, A. A., Abu-Dalu, M., Albadarneh, R. B., Abdallah, A. E., & Al-Hazaimeh, O. M. (2020). A new RSA public key encryption scheme with chaotic maps. International Journal of Electrical & Computer Engineering (2088-8708), 10(2).

[17] Satyanarayana, C., Rao, K. N., Bush, R. G., Patnala, B. D., & Kiran Kumar, R. (2019). A novel level-based DNA security algorithm using DNA codons. Computational Intelligence and Big Data Analytics: Applications in Bioinformatics, 1-13.

[18] Abdalrdha, Z. K., Al-Qinani, I. H., & Abbas, F. N. (2019). Subject review: key generation in different cryptography algorithm. International Journal of Scientific Research in Science, Engineering and Technology, 6(5), 230-240.

[19] Sivakumar, R., Balakumar, B., & Pandeeswaran, V. A. (2018). A study of encryption algorithms (DES, 3DES and AES) for information security. International Research Journal of Engineering and Technology (IRJET), 5(04).

[20] Vashi, D., Bhadka, H. B., Patel, K., & Garg, S.(2019) Performance of Symmetric and Asymmetric Encryption Techniques for Attribute Based Encryption.

[21] Dixit, P., Gupta, A. K., Trivedi, M. C., & Yadav, V. K. (2018). Traditional and hybrid encryption techniques: a survey. In Networking communication and data knowledge engineering (pp. 239-248). Springer, Singapore.

[22] Khan, M. A., Mishra, K. K., Santhi, N., & Jayakumari, J. (2015, April). A new hybrid technique for data encryption. In 2015 Global

[23] Stoyanov, B., & Nedzhibov, G. (2020). Symmetric key encryption based on rotation-translation equation. Symmetry, 12(1), 73.

[24] Qureshi, M. B., Qureshi, M. S., Tahir, S., Anwar, A., Hussain, S., Uddin, M., & Chen, C. L. (2022). Encryption Techniques for Smart Systems Data Security Offloaded to the Clo589+ud. Symmetry, 14(4), 695.

[25] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

[26] [Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. (2019). A novel block encryption algorithm based on chaotic S-box for wireless sensor network. IEEE Access, 7, 53079-53090.]

[27] Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.

[28] Gupta, D. R. (2020). A Review paper on concepts of cryptography and cryptographic hash function. European Journal of Molecular & Clinical Medicine, 7(7), 3397-3408.

[29] Khan, M. A., Khan, J., Sehito, N., Mahmood, K., Ali, H., Bari, I., ... & Ghoniem, R. M. (2022). An Adaptive Enhanced Technique for Locked Target Detection and Data Transmission over Internet of Healthcare Things. Electronics, 11(17), 2726.

[30] Jacak, M. M., Jóźwiak, P., Niemczuk, J., & Jacak, J. E. (2021). Quantum generators of random numbers. Scientific Reports, 11(1), 1-21.

[31] Conley, J. P. (2019). Encryption, Hashing, PPK, and Blockchain: A Simple Introduction. Vanderbilt University, Department of Economics.

[32] [Barani, M. J., Ayubi, P., Valandar, M. Y., & Irani, B. Y. (2020). A new Pseudo random number generator based on generalized Newton complex map with dynamic key. Journal of Information Security and Applications, 53, 102509.]

[33] Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. International Journal of Information Security, 1-19.

[34] Zebari, D. A., Haron, H., Zeebaree, S. R., & Zeebaree, D. Q. (2018, October). Multi-level of DNA encryption technique based on DNA arithmetic and biological operations. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 312-317). IEEE.

[35] Lin, K. N., Volkel, K., Tuck, J. M., & Keung, A. J. (2020). Dynamic and scalable DNA-based information storage. Nature communications, 11(1), 1-12.

[36] Sadkhan, S. B. (2021, June). Information Security based on DNA-Importance and Future Trends. In 2021 International Conference on Communication & Information Technology (ICICT) (pp. 310-314). IEEE.

[37] [El-Moursy, A. E., Elmogy, M., & Atwan, A. (2018). DNA-based cryptography: motivation, progress, challenges, and future. J. Softw. Eng. Intell. Syst, 3(1), 67-82.].

[38] M. Krajčovič, V. Hančinský, Ľ. Dulina, P. Grznár, M. Gašo, and J. Vaculík, "Parameter setting for a genetic algorithm layout planner as a toll of sustainable manufacturing," Sustainability, 11. 2083, (2019).

[39] Abood, O. G., & Guirguis, S. K. (2019). DNA computing and its application to information and data security field: A survey. DNA, 3(1), 1-5.

[40] Bhoi, G., Bhavsar, R., Prajapati, P., & Shah, P. (2020, December). A Review of Recent Trends on DNA Based Cryptography. In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) (pp. 815-822). IEEE.

[41] Kolate, V., & Joshi, R. B. (2021). An Information Security Using DNA Cryptography along with AES Algorithm. Turkish Journal of Computer and Mathematics Education, 12(1S), 183-192.

[42] Vinotha, P., & Jose, D. (2019, February). VLSI implementation of image encryption using DNA cryptography. In Intelligent Communication Technologies and Virtual Mobile Networks (pp. 190-198). Springer, Cham.

[43] Huo, D., Zhou, D. F., Yuan, S., Yi, S., Zhang, L., & Zhou, X. (2019). Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding. Physics Letters A, 383(9), 915-922.

[44] Microfluidic / https://www.ufluidix.com/resources/definitions/

[45] Wang, J., Rodgers, V. G., Brisk, P., & Grover, W. H. (2017). MOPSA: A microfluidics-optimized particle simulation algorithm. Biomicrofluidics, 11(3), 034121.

[46] Fuerstman, M. J., Garstecki, P., & Whitesides, G. M. (2007). Coding/decoding and reversibility of droplet trains in microfluidic networks. Science, 315(5813), 828-832.

[47] Datta, S., & Ghosal, S. (2009). Characterizing dispersion in microfluidic channels. Lab on a Chip, 9(17), 2537-2550.

[48] Lee, P. J., Hung, P. J., & Lee, L. P. (2007). An artificial liver sinusoid with a microfluidic endothelial-like barrier for primary hepatocyte culture. Biotechnology and bioengineering, 97(5), 1340-1346.

[49] Teh, J. S., Alawida, M., & Sii, Y. C. (2020). Implementation and practical problems of chaos-based cryptography revisited. Journal of Information Security and Applications, 50, 102421.

[50] Yager, P., Edwards, T., Fu, E., Helton, K., Nelson, K., Tam, M. R., & Weigl, B. H. (2006). Microfluidic diagnostic technologies for global public health. Nature, 442(7101), 412-418.

[51] Ma, P., & Sun, H. (2019, April). A New Molecular Encryption Model Based on Microfluidic Techniques. In Journal of Physics: Conference Series (Vol. 1187, No. 4, p. 042052). IOP Publishing.

[52] Muthu, J. S., & Murali, P. (2021). Review of chaos detection techniques performed on chaotic maps and systems in image encryption. SN Computer Science, 2(5), 1-24.

[53]. Sayan, H. H., & Ali, U. Z. U. N. (2021, December). Mask Based Image Encryption Using Chaotic Logistic Map. In 2021 1st International Conference On Informatics And Computer Science (p. 102).

[54] Özkaynak, F. (2020). On the effect of chaotic system in performance characteristics of chaos based s-box designs. Physica A: Statistical Mechanics and its Applications, 550, 124072.

[55] Sridevi, A., Sivaraman, R., Balasubramaniam, V., Siva, J., Thanikaiselvan, V., & Rengarajan, A. (2022). On Chaos based duo confusion duo diffusion for colour images. Multimedia Tools and Applications, 81(12), 16987-17014.

[56] Wang, L., & Cheng, H. (2019). Pseudo-random number generator based on logistic chaotic system. Entropy, 21(10), 960.

[57] Raghuvanshi, K. K., Kumar, S., & Kumar, S. (2020). A data encryption model based on intertwining logistic map. Journal of Information Security and Applications, 55, 102622.

[58] Wan, Y., Gu, S., & Du, B. (2020). A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. Entropy, 22(2), 171.

[59] Zubkov, A. M., & Serov, A. A. (2019). Testing the NIST Statistical Test Suite on artificial pseudorandom sequences. Математические вопросы криптографии, 10(2), 89-96.

[60] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

[61] Zhang, L., & Zhang, X. (2020). Multiple-image encryption algorithm based on bit planes and chaos. Multimedia Tools and Applications, 79(29), 20753-20771.

[62] Permana, A. A., Dewi, A. K., & Magfirawaty, M. (2020, October). True Random Number Generator Based on Wake-Up Ring Oscillator Utilizing Post-Processing Optimization to Generate Random Bit Sequence. In 2020 2nd International Conference on Industrial Electrical and Electronics (ICIEE) (pp. 149-152). IEEE.

[63] Zaman, J. K. M. S., & Ghosh, R. (2012). Review on fifteen Statistical Tests proposed by NIST. Journal of Theoretical Physics and Cryptography, 1, 18-31.

[64] Wang, X., Zhao, H., Feng, L., Ye, X., & Zhang, H. (2019). High-sensitivity image encryption algorithm with random diffusion based on dynamic-coupled map lattices. Optics and Lasers in Engineering, 122, 225-238.

[65] El-Latif, A. A. A., Abd-El-Atty, B., Belazi, A., & Iliyasu, A. M. (2021). Efficient chaos-based substitution-box and its application to image encryption. Electronics, 10(12), 1392.

[66] Hayouni, H., & Hamdi, M. (2021). A novel energy-efficient encryption algorithm for secure data in WSNs. The Journal of Supercomputing, 77, 4754-4777.

[67] Biyashev, R. G., Kapalova, N. A., Dyusenbayev, D. S., Algazy, K. T., Wojcik, W., & Smolarz, A. (2021). Development and analysis of symmetric encryption algorithm Qamal based on a substitution-permutation

network. International Journal of Electronics and Telecommunications, 67(1), 127-132.

[68] Verma, R., & Sharma, A. K. (2020). Cryptography: Avalanche effect of AES and RSA. International Journal of Scientific and Research Publications, 10(4), 119-125.

[69] Rajesh, S., Paul, V., Menon, V. G., & Khosravi, M. R. (2019). A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. Symmetry, 11(2), 293. .

[70] Liu, L., Zhang, Z., & Chen, R. (2019). Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos. IEEE Access, 7, 126450-126463.

[71] Abdulmehdi, N. A., & Kadum, S. A. (2021, March). Cryptanalysis Using DNA-Sticker Algorithm. In Journal of Physics: Conference Series (Vol. 1818, No. 1, p. 012088). IOP Publishing.

[72] Alsaffar, D. M., Almutiri, A. S., Alqahtani, B., Alamri, R. M., Alqahtani, H. F., Alqahtani, N. N., & Ali, A. A. (2020, March). Image encryption based on AES and RSA algorithms. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.

[73] Ali, H. J., Jawad, T. M., & Zuhair, H. (2021). Data security using random dynamic salting and AES based on master-slave keys for Iraqi dam management system. Indones. J. Electr. Eng. Comput. Sci, 23, 1018.

[74] Jiang, T., Luo, S., Wang, D., Li, Y., Wu, Y., He, L., & Zhang, G. (2023). A new bin size index method for statistical analysis of multimodal datasets from materials characterization. Scientific Reports, 13(1), 1-24.

[75] Liao, M., Zheng, S., Pan, S., Lu, D., He, W., Situ, G., & Peng, X. (2021). Deep-learning-based ciphertext-only attack on optical double random phase encryption. Opto-Electronic Advances, 4(5), 200016-1.

[76] Gohr, A. (2022). Brute Force Cryptanalysis. Cryptology ePrint Archive.

[77] Abdulmehdi, N. A., & Kadum, S. A. (2021, March). Cryptanalysis Using DNA-Sticker Algorithm. In Journal of Physics: Conference Series (Vol. 1818, No. 1, p. 012088). IOP Publishing.

الخلاصة

تزداد الشبكات المحلية والإنترنت يومًا بعد يوم ، ويتم نقل كمية كبيرة من المعلومات عبر هذه الشبكات كل يوم مما يؤدي إلى زيادة هائلة في تهديدات أمن المعلومات. لذلك ، كان من الضروري استخدام التقنيات التي تضمن أمن وسرية المعلومات المنقولة. لهذه الأسباب ، تم اقتراح العديد من التقنيات لحماية مثل هذه المعلومات مثل التشفير وإخفاء المعلومات لتحسين أمان نقل المعلومات عبر الإنترنت.

في الآونة الأخيرة ، دخل نظام الجزيء الحيوي في اتجاه الأمان ليلعب دورًا مميزًا في هذا المجال باستخدام تشفير الحمض النووي. مجال واعد في أمن المعلومات. فهو يجمع بين الحلول الكلاسيكية في التشفير وقوة المادة الوراثية. من خلال إدخال الحمض النووي في تشفير المفتاح المتماثل المشترك ، من الممكن الاستفادة من مزايا أنظمة التشفير الكلاسيكية وحل بعض قيودها. هناك طرق مختلفة لكيفية استخدام الحمض النووي لتأمين محتوى المعلومات. يتعلق الأمر باستخدام الوسط البيولوجي للحمض النووي لتخزين البيانات وإخفائها. يمكن وضع المعلومات السرية في الحجم المجهري للحمض النووي وإخفائها بين كمية كبيرة من هياكل الحمض النووي الأخرى. يمكن إجراء الحساب الجزيئي الحيوي باستخدام هياكل DNA المصممة خصيصًا. الأجزاء القيّمة من هذا النوع من الحسابات هي خاصية التجميع الذاتي لجزيئات الحمض النووي والحسابات المتوازية.

اقترحت هذه الأطروحة خوارزمية جديدة لتشفير تيار متماثل هجين تعتمد على تقنية ميكروفلويديك وتسلسل الحمض النووي ، وتتضمن الطريقة المقترحة ثلاث مراحل (توليد المفتاح ، والتشفير ، وعملية فك التشفير). المرحلة الأولى هي إجراء إنشاء المفتاح بناءً على السلوك غير الخطي لتقنية الموائع الدقيقة ، وتتألف من ثلاث خطوات: (إنشاء لوحة المفاتيح ، واختيار مفتاح البذور ، وتوسيع المفتاح)

المرحلة الثانية هي إجراء التشفير لتشفير الرسالة في تسلسل الحمض النووي باستخدام عملية XOR للحصول على نص تشفير قوي وآمن وغير قابل للكسر نسبيًا بتنسيق.DNA

المرحلة الثالثة هي إجراء فك التشفير لاسترداد الرسالة الأصلية عن طريق عكس عمليات التشفير.

أثبتت النتائج التجريبية للنظام المقترح كفاءة طريقتنا في تحقيق بُعد أمان قوي ومتعدد المستويات من خلال مجموعة من المقاييس مثل (تأثير الانهيار الجليدي (٧٨.٣٩%، ٦٥.١٣%، ٧٨.٢٨%) ، وقت التشفير (٠.١٠٤٣ ، ٠.٢٠٧٨ ، ٠.٣٠٢٢) ، وقت فك التشفير (٠.١٠٣٣ ، ٠.٢٠٥٦ ، ٠.٣٠٧٧) ، معدل النقل (٩.١٠٤٦ ، ٨.٨٨٩٩ ، ٦.٩٣٥١) , معدل الخطأ في البت (٠.٤٠١١،٠.٢٠٨٦، ٠.٥٥٩٧) لحجم الملف (١ كيلو بايت ، ٢ كيلو بايت ، ٣ كيلو بايت) على التوالي.

وزارة التعليم العالي و البحث العلمي
جامعة بابل كلية العلوم للبنات
قسم علوم الحاسوب

نموذج تشفير هجين يعتمد على تقنيات الجزيئية والموائع الدقيقة

رسالة مقدمة الى مجلس كلية العلوم للبنات في جامعة بابل وهي جزء من متطلبات الحصول على درجة الماجستير في علوم الحاسبات

مقدمة من قبل
هبة صفاء هاشم

بإشراف

د.سحر عادل كاظم
د.علي يعقوب السلطان

1444 هـ **2023 م**