COMPARATIVE STUDY OF POPULAR CRYPTOGRAPHIC TECHNIQUES

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

Master of Technology
in
Computer Science and Engineering

Under the esteemed guidance of
Sonika Dahiya
Assistant Professor
Computer Science and Engineering
Delhi Technological University

Submitted By-
Ruchi Sharma
(Roll No. - 2K16/CSE/11)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

SESSION: 2016-2018

CERTIFICATE

This is to certify that report entitled Ruchi Sharma (2K16/CSE/11) has completed the thesis titled "**Comparative Study of Popular Cryptographic Techniques**" under my supervision in partial fulfilment of the MASTER OF TECHNOLOGY degree in Computer Science and Engineering at DELHI TECHNOLOGICAL UNIVERSITY.

Assistant Prof. Sonika Dahiya
Department of Computer Science and Engineering
Delhi Technological University
Delhi -110042

DECLARATION

We hereby declare that the thesis work entitled "**Comparative Study Of Popular Cryptographic Techniques**" which is being submitted to Delhi Technological University, in partial fulfilment of requirements for the award of degree of Master of Technology (Computer Science and Engineering) is a bonafide report of thesis carried out by me. The material contained in the report has not been submitted to any university or institution for the award of any degree.

Ruchi Sharma
2K16/CSE/11

ACKNOWLEDGEMENT

First of all, I would like to express my deep sense of respect and gratitude to my project supervisor Assistant Prof. Sonika Dahiya for providing the opportunity of carrying out this project and being the guiding force behind this work. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

Secondly, I am grateful to Dr. Rajni Jindal, HOD, Computer Science & Engineering Department, DTU for her immense support. I would also like to acknowledge Delhi Technological University library and staff for providing the right academic resources and environment for this work to be carried out.

Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.

Ruchi Sharma

ABSTRACT

In computer network, information has been broadly exchanging over the communication system but the security over the communication system is not very sufficient and the data can be breached by interceptors. To provide security over the communication system, cryptography technique is used to provide more security to the data. In this process, the primary information is changed over into jumbled data with the help of key. DNA cryptography is preferred to be highly secure technique than other cryptographic techniques due to its vast parallelism and a enormous amount of data can be inherit in any DNA molecule. In this paper, various cryptographic techniques have been implement on different strings having different patterns.

TABLE OF CONTENTS

FIGURES AND TABLES

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION

With the developing pace of web and system innovation step by step, the security treats are likewise expanding for the clients, because of part of information stream on the system. There are different foes who dependably attempt to break into the framework with a specific end goal to take the pivotal information or to crush the integrity of data. Along these lines, information security moves toward becoming need for current processing frameworks. There are a few segments like government, banks, military who can't manage the cost of any breaks to their secret data. From our past to till date the secret written work procedure are utilized to shield the data from e enemies and the strategies, for example, cryptography and steganography are most normal and broadly utilized techniques. Cryptography plays out the encryption of the data though steganography conceals the data from the programmer. In cryptography, encryption and decryption of the data is finished with the assistance of key.

The most secure and by and by utilized technique is the cutting edge strategies for cryptography which includes much numerical calculations and two sorts of keys, the public key and the private key. These days, there is another recently developing cryptographic technique in the field of cryptography called DNA cryptography. The principle goal of this strategy is to scramble the plaintext and shroud it in digital form. DNA cryptography empowers the secrecy of information all the more high then the cutting edge strategies with the utilization of one time pad keys and its size. Additionally, it is trusted that in DNA cryptography the key can be created for the length of information contrasted with the advanced strategies in which key are produced just for smaller length of the information.

For couple of years prior making utilization of 56 bit encryption appeared to be sheltered everlastingly yet as the registering force and learning of man expanded these encryption plots additionally vanished. So with the failure of present day cryptographic calculation like DES and MD5, new strategies for data security are expected to ensure our information.

Researchers and mathematicians are ceaselessly endeavoring to improve the encryption techniques while remaining inside the cutoff points of innovation accessible to us. Encryption calculation RSA which depends on public key cryptography has been not split yet by anybody but rather future we can't anticipate. The idea of DNA processing give us a beam in the field of PC security which is guaranteed to be an all the more powerful and unbreakable cryptographic calculation now a days. With the assistance of DNA figuring, Adleman and Lipton tackled the combinatorial problems like Hamiltonian way and fulfillment issue. Besides the combinatorial problems DNA registering has numerous energizing applications for cases DNA and RNA can store extensive measure of information in a smaller volume. They limitlessly surpass the limit of the other storage mediums, for example, electronic, attractive and ideal medium. A gram of DNA can store 10^{21} DNA bases or around 10^{8} TB[1]. Henceforth, a couple of gram of DNA can store every one of the information around the globe. Disregarding its points of interest, it has additionally a few disadvantages, for example, the necessity of most extreme calculation time, hi tech bimolecular lab and high computational many-sided quality.

1.2 CRYPTOGRAPHY

In computer network, data has been broadly exchanging over the communication system but the security over the communication system is not very sufficient and the data can be breached by interceptors. So, the ability to protect and secure data which has been sent from one user to another user is becoming necessary to the growth of electronic commerce, social media, information and data sharing etc. This data sharing should be safe and secure.. So, this has led to the growth of many modern cryptography techniques which are based on many algorithms and mathematical theories. To provide security over the communication system, cryptography technique is used. Generally, Cryptography is the training and investigation of methods for secure correspondence within the sight of untouchables called foes. It includes making composed or created codes that enable data to be kept mystery. It changes over information into an organization known as cipher text that is confused for an unapproved client, enabling it to be transmitted without unapproved substances having the capacity to peruse it. This procedure of changing plaintext to cipher text is known as encryption and the other way around is known as decryption.

Every single cryptographic procedure are extensively sorted as Symmetric cryptography and asymmetric cryptography. In symmetric cryptography, both sender and collector utilizes a solitary key for encryption and in addition decryption and in asymmetric cryptography, public key is used by the sender to scramble the message and the private key is used by the beneficiary to unscramble the message.

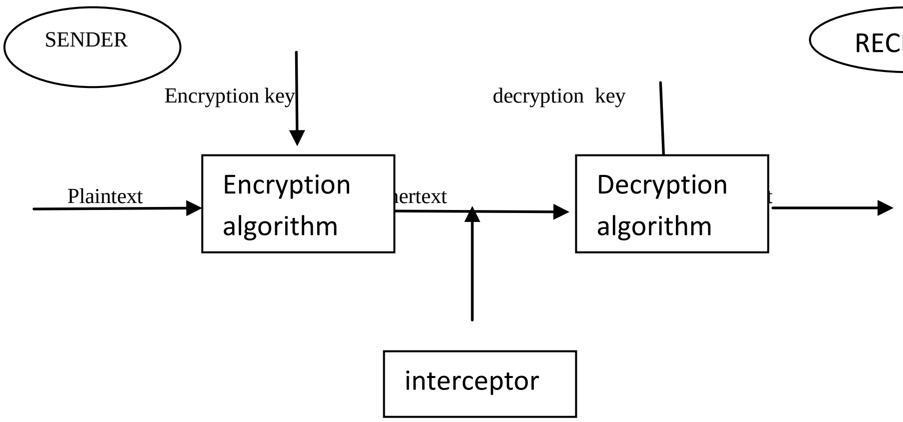

Fig 1.1 Flow Diagram of Cryptography

Plaintext sent by a sender to receiver has to be protected during the whole transmission from an inceptor or from an attacker or from an unauthorized party which tries to determine the data. So, in order to protect the data encryption algorithm is applied on a given plaintext along with the encryption key which is a value that is known only to sender and sender uses this key along with plaintext to compute the cipher text and to decrypt the cipher text, there is a decryption algorithm which is also a mathematical process which uses the cipher text along with decryption key which is a value that is known only to receiver and receiver uses this key to compute the plaintext. This algorithm takes cipher text and decryption key as an input and then produces the output i.e., plaintext.

1.3 GOALS OF SECURITY

Security consists of various goals but among these common and noticeable one lies in CIA i.e. Confidentiality, Integrity and Availability.

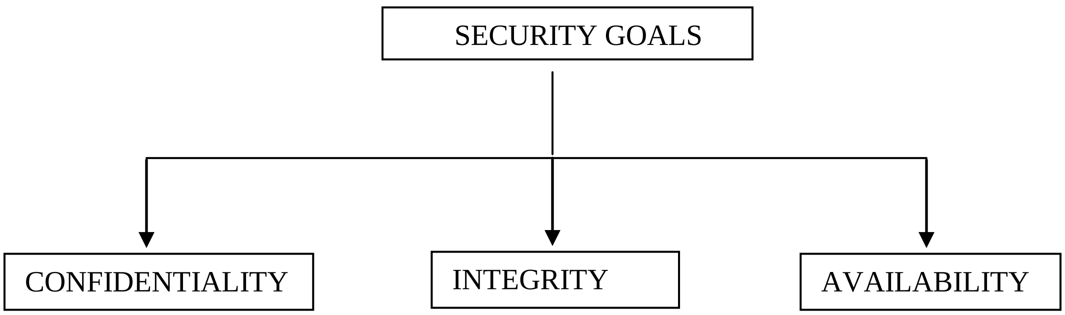

Fig 1.2 Main goals of security

- Confidentiality: Hiding/keeping data from enemies/unapproved client.
- Integrity: Preventing data/information from change by the enemy.
- Availability: Resources ought to be accessible to the approved clients.

1.3.1 Threats to Confidentiality

- Snooping: It alludes to the unapproved access or block attempt of data, with the assistance of some observing instruments like as key logger or eavesdropping.
- Traffic Analysis:

  Traffic Analysis concentrates on the communication patterns between the parties in a system. In order to decipher information from patterns in communications, the process of traffic analysis involves intercepting and examining of messages.

1.3.2 Threats to Integrity

- Modification: In this assailant will modify the information which is send by the sender, with the goal that the recipient will get wrong information/result.
- Masquerading: In this caricaturing assaults are performed by the assailant, with the goal that the sender and receiver traffic will go through the aggressor.

1.3.3 Threats to Availability

- Denial of services: Creating parcel of traffic to the objective or expending the network bandwidth by aggressor to such an extent that the planned receiver won't get the coveted asked for service around then.

1.4 ATTACKS ON CRYPTOSYSTEM:

In the modern era, all the aspects of human life are driven by data. Along these lines, it is vital to shield helpful data from malignant exercises, for example, attacks. In this way, attacks are regularly arranged based on activity performed by the assailant. In this manner, an assault can be passive or active.

1.4.1 PASSIVE ATTACKS:

The primary point of this kind of attack is to acquire unapproved access to the data.The goal of the opponent is to obtain information that is being transmitted. Actions like intercepting and eavesdropping are considered to be an passive attacks. Passive attacks are of two types: release of message contents and traffic analysis.

A telephonic conversation, an electronic mail message and a transferred file may contain some confidential information and an unauthorized party can easily understand the release of the message content. So, it is necessary to prevent an opponent from learning the contents of these transmissions. Traffic analysis is a type of inference attack. This type of attacks mainly concentrates on the communication patterns between the parties in a system. In order to decipher information from patterns in communications, the process of traffic analysis involves intercepting and examining of messages.

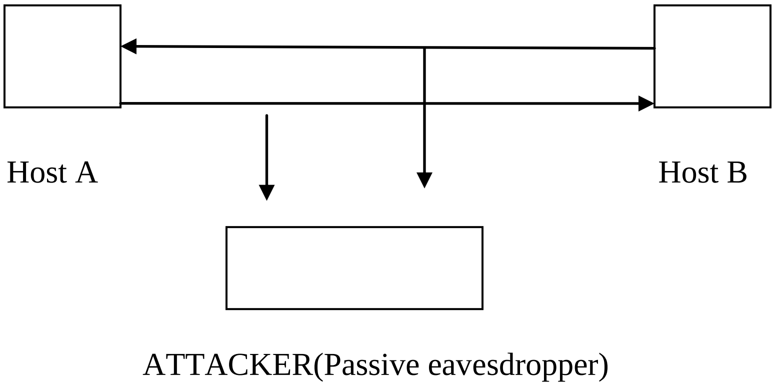

Fig. 1.3 Flow Diagram of Passive Attacks

1.4.2 ACTIVE ATTACKS:

An active attack includes changing the data somehow by leading some procedure on the data like adjusting the data in an unapproved way, starting unintended or unapproved transmission of data, alteration with verification data like with originator name or timestamp related with data, unapproved erasure of data or foreswearing of administrations.

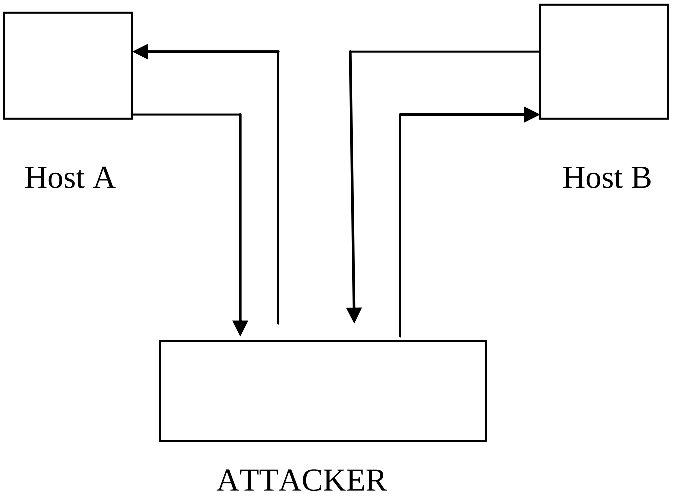

Fig 4. Flow Diagram of Active Attacks

1.5 **COMMON CRYPTOGRAPHY ATTACKS:**

1 Cipher text –only attack:

It is a standout amongst the most troublesome cryptography attacks in light of the fact that in this, assailant does not have much data when they begin, along these lines, all aggressor begins with some incomprehensible data that may suspects some imperative encrypted message. In the event that the aggressor can assemble a few bits of cipher text, at that point the assault winds up basic for the assailant.

2. Known Plain text:

The objective of this assault is to locate the cryptographic key that was utilized to scramble the message. In this way, for this, the aggressor needs to get to both the cipher text and the plain text variant of a similar message.

3. Chosen Plain text:

   In this assault, assailant knows the algorithm which has been utilized for the scrambling then he can endeavor to get to the machine used to do the encryption and attempting to decide the key.

4. Chosen Cipher Text:

   It is fundamentally the same as chosen plain text. In this assault, attacker approaches the decryption gadget or programming and is endeavoring to crush the cryptographic insurance by decoding chosen bits of cipher text to find the key.

5. Different Cryptanalysis:

   These sorts of assaults are executed by estimating the correct execution time and power required to perform encryption and decryption by the crypto gadget. It is likewise called side channel assault.

6. Implementation Attacks:

Because of their straightforwardness on framework components of the algorithm, usage attacks are a portion of the prevalent attacks against cryptographic framework. Some execution attacks are-

i. Side Channel attacks: These kinds of attacks rely upon the physical trait of the usage, for example, control utilization and after that utilization these ascribes to decide the algorithm and secret key utilized.

ii. Fault Analysis: These attacks endeavors to drive the framework into a blunder state to increase incorrect outcomes. By driving a blunder, the attacks can pick up the outcomes and by contrasting it and some great known outcomes, at that point the aggressor may find out about the secret key and algorithm utilized.

iii. Probing Attacks: These kinds of attacks are endeavored to watch the hardware encompassing the cryptographic module with the expectation that the any corresponding part will uncover the data about the key or the algorithm utilized. Moreover, any new equipment can be added to the cryptographic module to watch and infuse data.

7. Replay Attack:

   This assault is intended to disturb and harm preparing by the aggressor through the resending of rehashed files to the host. On the off chance that there are no checks, for example, time stamping, utilization of one-time tokens or succession confirmation codes in the getting programming, the framework may process copy files.

8. Dictionary attacks:

   It is a standout amongst the most well-known attacks against password files. It misuses the poor propensities for clients who pick straightforward password in light of regular words. This assault encrypts the greater part of the words in a dictionary and after that checks whether the subsequent hash coordinates an encoded password put away in the SAM document or some other password record. SAM record remains for Security Accounts Manager which is a database in the windows OS that contains client names and passwords. It is a piece of the registry and can be found on the hard circle.

9. Brute Force:

This assault attempts all conceivable keys until the point that one key is discovered that unscrambles the figure content. That is the reason key length is considered one of the imperative factors in deciding the quality of the cryptosystem.

10. Timing Attacks:

They misuse the way that each calculation take diverse circumstances to figure on processor. Along these lines, by estimating such timings, it is feasible for an assailant to think about a specific calculation the processor is doing. For instance, if the,encryption takes a more drawn out time, it shows that the secret key is long.

1.6 TRADITIONAL CIPHERS:

The goal of traditional cipher is to arrange a plaintext in such a way that any interceptor of that cipher text can't guess the cipher text.

Traditional cipher is of two types:

1.6.1 Substitution Cipher:

In substitution cipher, one letter of the cipher text is replaced with any other letter.
Some substitution ciphers are:

i. Monoalphabetic Cipher:

sThe relationship between a symbol in a plaintext to a symbol in a cipher text is always one to one.

Example: Plaintext: CRYPTOGRAPHY

Cipher text: DVGSXZIVHSAG

ii. Additive Cipher:

Each coded letter is essentially moved a specific number of spaces from the plain text letter.

Example: Plaintext: CRYPTOGRAPHY

Mathematical Equation: $(P+K_1-K_2)$ mod 26

Cipher Text: RGNEKDVGPEWN

iii. Multiplicative Cipher:

In this, encryption algorithm is specified by multiplying key with the plaintext and the decryption algorithm is specified by dividing key with the cipher text.

Example: Plaintext: CRYPTOGRAPHY

Mathematical Equation: $C=(p*k)$ mod 26

key =2

Cipher Text: EIWEMCMIOEOW

iv. Affine Cipher:

It is a combination of both the ciphers with a pair of keys.

Example: Plaintext: CRYPTOGRAPHY

Mathematical Equation: $C=(p*k_1+k_2)$mod 26

$P=((c-k_2)*k_1^{-1})$ mod 26

Where $k_1=7$, $k_2=2$

Cipher Text: QRODFSRCDZO

v. Polyalphabetic Cipher:

Each occurrence of a character may have a different substitute.

Example: Plaintext: CRYPTOGRAPHY

Mathematical Equation: $C_i=(p_i+k_i)$ mod 26

$P_i=(c_i-k_i)$ mod 26

Keyword=CIPHER

Cipher Text: EZNWXFIZPWLP

vi. Playfair Cipher:

At first a key table is made. The key table is 5*5 which go about as a key for encrypting the plaintext. Every one of the 25 letters in order must have a special and a letter of the letter set is discarded from the table as we just need 25 letters in order.

Example: Plaintext: CRYPTOGRAPHY

Keyword: MESSAGE

Cipher text: DQVTUNSUMTEZ

vii. Vignere Cipher:

In this, the letters are shifted by different amounts.

Example: Plaintext: CRYPTOGRAPHY

Mathematical Equation: $C_{i=}P_i+K_i$ $P_i=C_i-K_i$

Keyword=cipher

Cipher text: EZNWXFIZPWLP

viii. Caesar Cipher:

It is a substitution cipher where each letter in the plaintext is supplanted with a letter relating to a specific number of letters up or down in the letter set.

Example:

Plaintext: CRYPTOGRAPHY

Mathematical Equation: $E_n(x)=(x+n)\text{mod } 26$ $D_n(x)=(x+n)\text{mod } 26$

Cipher text: HWDUYTLWFUMD

1.6.2 Transposition Cipher:

In transposition cipher, it changes the location of symbols of plaintext.

Transposition Cipher is further of two types:

i. Keyless Transposition Cipher:

In this, the message to change over to cipher text by both of two permutation technique: a) text is built into a table row by row and is then transmitted column by column. b) Text is built into a table column by column and is then transmitted row by row.

Example:

Plaintext: CRYPTOGRAPHY

Cipher text: CYTGAHRPORPY

ii. Keyed Transposition Cipher:

In this, the entire plaintext is divided into the block of predetermined size and then each block is permute independently.

Example:

Plaintext: CRYPTOGRAPHY

Cipher text: POAPCYTRGYRH

1.7 APPLICATIONS OF CRYPTOGRAPHY:

Cryptography plays an important role in many IT applications. Let's discuss various applications of cryptography and its intersection with computer science.

1. Time Stamping:

   It is a technique that affirms that a specific report or any sort of correspondence was made and was conveyed at a specific time. This uses blind signature conspire as an encryption demonstrate.

   Blind signature enables the sender to get a message recognized by another gathering without uncovering any data to the unapproved party.

2. Electronic Money:

   This application includes transactions of funds from one party to another party electronically i.e. internet. These transactions can be done either by debit card or by credit card and can be either identified or anonymous. There are both hardware and software implementation of electronic money.

   Encryption in this scheme is used to secure transaction data like transaction amount, account number. This can also be done by just replacing credit card authorizations or hand written signature by digital signature.

3. Secure Socket Layer(SSL):

   This protocol is used for giving information security between TCP/IP. It supports data encryption, server authentication, message integrity, confidentiality for TCP/IP connections.

   Thus, protocol authenticates both server and client with the second server or client authentication. In phase 1, the receiver requests for the server's certificates and its cipher preferences. In the wake of getting the data from the server, the recipient produces a master keys and the encrypt it with the assistance of server's open key and afterward it sends the master key back to the server. The server decodes the master key with its private key and after that sends the recognize the collector by sending the message encrypted with master key.

SSL uses the RSA algorithm for the authentication steps and after exchanging of keys. Various algorithms like RC2, RC4, IDEA, and triple DES are used.

4. Strong Authentication:

Authentication is the process in which the claimed identities of the users are verified to some degree of certainty. When the authentication completed successfully then only other processes can take place. There are various different methods are included in authentication like from simpler user name/password to advanced biometrics pattern recognition.

4.1 Multi factor:

In this, the various different factors of the claimed users is combined which provides strengthen to the authentication process.

The authentication factor includes:

i. Something that is only known to the user like password or security code.

ii. Something that user has like any kind of document or a hardware taken of some kind.

iii. Something the user is: e.g. biometric features like fingerprints, retina, face or ear features.

It is believed that combination of any two out of above three categories works best.

4.2 Multi-Channel:

Authentication can be achieved by just providing a extra separate cannel to the claimed user or by sending OTP to the customer for signing on to the service. It is believed that the extra channel cannot be eavesdropped on by an attacker. When the user signs on the user, a list of code is distributed to the user in advance and these codes are sent over a different channel during the authenticable process.

4.3 Tamperproof Network:

In this case, the key is hold by the hard disk of the user’s desktop or computer. So, in this case, if the attacker resides on the network then it is not the big issue. But this situation changes if the desktop or computer of the user is shared by different users which cannot be trusted. So, the attacker might install malware on the user's desktop or computer. So, in respect to provide security in such cases, special cryptographic tokens like PKI token or smart cards are utilized to hold the private key of user. The private key is utilized by the hardware itself during a challenge response protocol but never leaves the cryptographic hardware. But, if the hardware is tamperproof, then if the user is not trusted then also, it can be used in an attacker model.

4.4 One time password generating tokens:

One time password is a password which is substantial for just a single login session or only for one transaction. The transaction will be successful if the OTP is recognized by the verifying party as valid and cannot be guessed by the unauthorized party. Password generators form class of network tokens then uses the cryptography in order to generate the session passwords. Internally, these tokens have a clock whose value is hashed and encrypted using a key which is shared with the verifying party.

RSA, VOSCO, Todos are some major authentication token manufactures that make such tokens. So, the OTP tokens are a very efficient way for securing the authentication to VPNs.

4.5 Challenge-Response tokens:

In this authentication scenario, a token that holds a cryptographic key is given to each user and the possession of the embedded key is proofed with the help of challenge response protocol.

The challenge response tokens typically require the user to enter the key into the token which has a keypad and a display. After this, the response is shown by the display and the user has to type this code into the webpage of service provider.

1.8 APPLICATIONS OF CRYPTOGRAPHY IN REAL LIFE

1.8.1. Cryptography techniques used in solving security issues in mobile computing

In 2015, Raghav Mathur, Shruti Mathur and Vishnu Sharma[10] have talked about the security issues emerging from the mechanical advances in mobile figuring and in addition their answer and execution. Symmetric algorithms like AES perform encryption and decryption in relatively less measure of time upgrading the wellbeing of information while exchanging the information over the air. Asymmetric algorithm like RSA and Diffie-Hellman are secure concerning their size of the keys. RSA corrects the issue of the key assention and key trade in secret key cryptography. Subsequently, the component of private and open keys can be incorporated from RSA algorithm in AES which can all the while give the advantage of quick encryption/decryption and more security than symmetric-key algorithms. They have additionally reasoned that The cryptographic algorithms give security however it can't ensure 100 percent wellbeing. Subsequently, the encryption as well as secure transmission of information over the system is obligatory. Right off the bat, in the event that anybody endeavors to make association with the sender or beneficiary amid the procedure of encryption and decryption, firewall can be given to hinder the interloper from assaulting. Besides, amid transmission of encrypted message, the message can be broken into parts and be sent to various distinctive mobile stations from where onwards it can be conveyed to recipient and simply in the wake of verifying the collector; it is brought together to the first message. It will save the secrecy of the message. Besides, the message and key which is sent can be comparable in frame to confound the assailant amongst key and message.

1.8.2. In enhancing security of images:

In 2016, Sadaf Bukhari, Muhammad Shoaib, M.R. Anjum, Samia Dilbar[11] gives a strategy to the security of picture in open remote channel. In this system, the fundamental progress is to cover a message picture inside an another encoding procedure which is double random stage encoding(DRDE) is perform on stego picture to incorporate more randomness in the stego picture and make it more secure for transmission. This technique works by supplant two or three the information in a particular pixel with the information from the data in the picture. LSB introducing system is perform on the minimum critical piece. By using this, base refinement in tints is made. In this strategy, they proposed a computation for an encryption of stego picture. Basically, this method first uses the two pictures, one is message picture and other is the cover picture. Through using the LSB stenography method, the stego picture is confined by inserted the message picture into discretionary picture. In second step, a stego picture is divided into 8*8 squares. The divided stego picture is mixed by double random stage encoding. In the wake of playing out various tests in MATLAB to evaluate the execution of proposed technique for transmission purpose behind picture through unsteady channel and its results are differentiated and the crypto structure which relies upon DCT and double random stage encoding. Diverse accurate tests like entropy, time investigation and PSNR(peak to signal noise ratio) with and without tumult are performed to survey the nature of proposed system. Along these lines, it is done up from the recreation and the investigation comes to fruition that the system improves the security of pictures when transmitted in remote correspondence condition against noise.

1.8.3. In Image Based Authentication Technique:

In 2017, V.Annie Daisy, C.Vijesh Joe, S.Shinly Swarna Sugi[12] has used visual cryptography for this reason. Visual Cryptography is a strategy which is used to shield the picture from being seen, subsequently, the mystery picture is apportioned into parts and after that each part is scattered to the various recipients. Thusly, the individual who has each one of the parts can simply unscramble the picture. In this way, they have used a visual cryptography conspire half conditioning figuring is used to isolate the mystery picture into parts with the help of Jarvis Filter. In this n-out – of-n VCS, a mystery picture is scrambled and unscrambled among all. The mystery picture can be revealed basically after the stacking of the entire offer. In Encryption process, it uses a variable number of LSBs from each pixel to cover, where the amount of bits perused each pixel shading i.e., red, green and blue phenomenal. Pictures in other shading design may be changed over to Red-Green-Blue (RGB) systems and changed over back after the masking is done. The genuine number of bits changes as demonstrated by neighborhood information of each pixel shading. Exactly when the similarity between a pixel shading and it neighbors is high, the pixel is set in a smooth domain where change will be distinguished easily. In this way, the amount of bit used for stowing endlessly is been conversely relating to the neighbor's typical estimation of each pixel shading. In Decryption Process, the extraction strategy glances through each one of the three grids, encountering all lines in each line and section a sequestered from everything technique. The amount of bits used for covering in a section, Org (row,col) is moreover directed by taking a gander at avg; the typical of the four neighbors as in the disguising technique. In case avg is greater than 2NLSBs+1, there is a regard masked in the segment, which is [Org (push col)- ave+2numLSBs]. The hidden regard are isolated and a short time later connected to shape the principal message. Along these lines, the proposed mystery sharing plan satisfies the four general conditions of security, computational flightiness and offer size and accuracy.

1.8.4. In Combinatorial Optimization

In year 2017, Karlo Knezevic[13] has used the concept of cryptography in combinatorial optimization. Combinatorial Optimization is a concept in which we have to find the optimal object from the finite set of objects.So, for this purpose, Karlo Knezevic has used Evolutionary computation algorithms which by and large speak to a scope of critical thinking procedure in view of standards of biological advancement and such algorithms can be utilized to take care of an assortment of troublesome issues, among which are those from zone of cryptography and which can be represented as combinatorial optimization problem.Evolutionary computation is a family of algorithms inspired by biological evolution, and the subfield of artificial intelligence and soft computing. It can roughly divided to three groups: evolutionary algorithms, swarm algorithms and other algorithms. Evolutionary algorithms could be broadly divided into 4 different approaches: genetic algorithms, genetic programming, evolutionary strategies and evolutionary programming. All of these algorithms have been successfully applied to the variety of problems in the field of combinatorial optimization. Evolutionary algorithms are based on the Darwinian theory of evolution. Main difference between all evolutionary algorithms is the way of individual encoding and evolutionary operators implementation. Swarm algorithms consist of ant algorithm, particle swarm algorithm, bee algorithms and others. Some swarm algorithms are inspired by experiments made by biologists or by software imitation of swarms in computer graphics. Common to all algorithms is a swarm population consisting of individuals of different individuals. Other algorithms are artificial immune system algorithms and cellular evolutionary algorithm. Each of these algorithms are specific and have different individual encoding or solution finding method.

1.8.5. In Color Share Generation:

In 2016, Trupti Patel and Rohit Shrivastava[14] have associated a visual cryptography to encode a shading picture as opposed to greyscale picture or binary picture. In this, shading picture is taken as a commitment to the system then they expel the R, G and B component from shading picture. After extraction organize dark offer age counts is associated on just R component and make n number of R dim offers. In following stage, they have joined B and G component with all made R dim offers to make shading shares. In decryption process, they evacuate the B and G component from all offers to make R dim offers then all R dark offers goes to dim offer age figuring and deliver R component. After this movement R component is join with B and G component to reveal the first mystery picture. Here, they have associated dim offer age computation on R component and produces the offer and after that combine with B and G components to make shading shares, so the security of mystery picture is extended by various wrinkle.

1.8.6. In IoT Environment:

In 2016. Ria Das and Indrajit Das[15] have utilized cryptography procedures for anchoring information move in IoT environment. Web of Things for the most part alludes to situations where organize network and processing capacity stretches out to people, remote identifiable articles, sensor, sensor embedded – shrewd small gadgets and ordinary things empowering these to produce, trade and devour information with insignificant human intervention.For this reason, Ria Das and Indrajit Das has consisdered sensor gadgets as the IoT gadgets which are in charge of detecting information from the environment in which it is conveyed and after that transmitting the detected information to the home server.

The previously mentioned security model can be unified into the accompanying two sections:

1. Amid the information transmission stage between IoT gadget and the confirmation/home server, the mix of stenography and a lightweight cryptographic procedure technique is proposed since we know about the way that IoT gadgets have natural equipment limitations, for example, constrained memory, battery control confinements, low computational capacities and in this way are wasteful to process computationally escalated and complex encryption algorithms.

2. Amid the information transmission stage between home server and the mists, a coordinated approach of stenography and standard, secure encryption algorithms, for example, AES/DES is received since here we have no such asset related imperatives.

The fundamental worry here is the dispatch of any digital assault by malevolent people, for example, spying/parcel sniffing, essentially in the LAN organize that catches the privacy of transmitted data. The purposed conspire which guarantee the unwavering quality of transmitted touchy information/data utilizing IoT gadget. The means are examined beneath:

stage 1: At the site of sensor(IoT gadget): a. The detected information is scrambled utilizing a lightweight encryption system before sending information to the home server specifically.

b. Next the message process of the detected information is registered utilizing Message Digest 5(MD5) algorithm.

c. In conclusion the encoded information form and processed process is hidden in a haphazardly chosen picture method to deliver another picture which is then exchanged to the home server for verification reason.

Stage 2: At the site of Home/Authentication server:

a. Applying reverse stenography system, the home server right off the bat acquires the embedded message process and the encoded information form.

b. At that point it decrypts the scrambled information form to recover the first detected information.

c. At long last in the wake of registering its message process, it contrast the recently figured process and the got process; if just match happens then information honesty is saved and effective validation happen else information is disposed of by it.

Stage 3: Similar to the approach laid out above in stage 1, amid the information transmission stage between the home server and the mists, a similar maker is repeated here by essentially supplanting the proposed lightweight encryption plot above by standard solid encryption algorithm, for example, AES/DES and basic LSB substitution method alluded above by recently purposed MSB-LSB substitution system.

1.8.7. For Securing Forensic Biometric Image Data:

In 2014, Quist-Aphesti Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, J.M Eghan, Nii Narku Quaynor[16] have proposed an approach of encryption for anchoring measurable biometric image data utilizing AES and visual cryptography. The encryption is finished by drawing in visual cryptographic system in view of image shares and transposition of the offer. A key is extricated from the image and after that scrambled utilizing AES before utilizing its commitment in the encryption procedure, it has been watched that there was no pixel development subsequently there was no misfortune in image quality. In an outcome and investigation, AES only permits a 128 bit data length that can be isolated into four fundamental task squares. Each cipher created by AES utilizes a few rounds of settled tasks to accomplish wanted yield which decides its security level which is estimated as far as dissemination and perplexity henceforth the quantity of round are picked with the end goal that the algorithm gives the SAC value.

1.8.8. In system secuirty for small and medium enterprises:

In 2013. Georgiana Mateescu and Marius Vladescu[17] have broke down these three figures: symmetric, asymmetric and hash function. To finish up, they purposed a hybrid approach of the exhibited cryptography which consolidates them for taking advantages from the greater part of their qualities and endeavors to diminish however much as could be expected the shortcoming of one method with the preferred standpoint in the accompanying way:

- The first's message digest is digitally signed.

- Symmetrical figure is utilized to code the first message. The secret key is acquired utilizing a key generator and it is occasionally changed.

- The private key utilized for symmetric figure is coded utilizing additionally RSA algorithm, however with various keys.

- The coded private keys is connected to the encrypted message together with the computerized signature.

1.8.9. In Wireless Sensor Network:

In year 2014, R.Selvam and Dr. A. Senthil kumar[18] resuscitate the cryptography based multipath routing protocols from mooring the information in remote sensor structures. The standard cryptography system can't finish unscramble in the remote sensor arrange by virtue of less power and vitality factors. In the nonstop examination result shows up, the security can be enhanced utilizing balanced cryptography algorithm in the sensor arrange.

CRYPTOGRAPHY BASED SECURE MULTIPATH ROUTING PROTOCOL

I. EENDMRP

Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) finds the unmistakable courses between the source and target in context of the rate of energy utilize. It utilizes a crypto structure which utilizes MD5, hash work and the RSA public key calculation. The public key appropriated uninhibitedly and private key scattered for every node. It has course headway orchestrate. Information transmission mastermind and transmit the information in remote sensor form.

ii. Dynamic Router Selection and Encryption for Data Secure In Wireless Sensor Network

Dynamic Router Selection and Encryption for Data Secure In Wireless Sensor Network propose randomized multipath courses which get ready for disavowal of association and wrangled node assaults. The algorithm utilizes symmetric key encryption to scramble the every single bundle before conclusion and unscramble resulting to getting the gatherings. It in like way utilizes RSA public key algorithm for encryption and unscrambling of the information. It utilizes three stage for tying down the information in WSN, mystery sharing of information, randomized development of every datum offer, and traditional routing. The baffle sharing stage the information separate into different offers and spread into the optional neighbor list.

iii. mEENDMRP

Multipath routing custom suggested for remote sensor arrange sharing the store between the sensor nodes and expansion the lifetime of the system. The changed Energy Efficient Node Disjoint Multipath Routing Protocol (mEENDMRP) depends upon the Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) and has course headway finding the node disjoint distinctive way and secure the information transmission stages. It utilizes low transmission go which diminishes the energy while transmitting the information.

iv. Security protecting and change in accordance with non-essential disappointment protocol

Security protecting and change in accordance with non-essential disappointment protocol utilizes efficient key cryptosystem. The mixed sensor information sending with multipath routing protocol see the error message and handle the copy message. Every sensor scrambles the message and totaled using Cascaded Ridesharing Protocol.

v. SCMRP

The Secure Cluster Based multipath routing protocol utilize blend of bundle based routing and multipath routing for getting the two inclinations. The SCMRP is a proactive kind protocol which recommends every last one of the courses are enrolled before they require. The advantage rich base station forms every single one of the courses. It has five specific stages.

1. Perceive the neighbor and produce the system topology.

2. Unite able key dispersal.

3. Gathering change

4. Information transmission

5. Re grouping and re-routing.

vi. Probabilistic multi-path redundancy transmission (PMRT)

Probabilistic multi-path redundancy transmission (PMRT) utilize ID based key association plot for perceiving wormhole ambushes. ID based key association protocol utilizes open key pre scattering plot. Each inside point passes on something specific and make the optional number and total. On the off chance that the total is more than the edge by then encode the message and send to a neighbor. The server keeps up the routing information. The outside assailant can't trap without the key. The server looks measure of shape information which keep inside attacker.

vii. Secure Routing and Broadcast Authentication in Heterogeneous Sensor Network:

Secure Routing and Broadcast Authentication in Heterogeneous Sensor Network propose secure routing for more secure and versatile heterogeneous sensor create. Base station make the routing table for cover assemble focus point and bundle focus make cover cluster routing tables which diminish the computational load on amass focus point. It has two stages, course introduction and information sending.

viii. SecSens-Security Architecture for Wireless Sensor Networks:

Security Architecture for Wireless Sensor Networks gives security partitions and heterogeneous sensor deal with. It utilizes for segments which cooperate with each other in giving security in sensor deal with. Checked pass on, key estimation, guiding and enroute isolating. SecSens utilizes initiation work keys, coordinate – savvy shared keys, bundle keys, total keys to satisfy troublesome security fundamentals.

ix. Prepare for Laptop Class Attacker:

Prepare for Laptop Class Attacker in remote sensor make utilizes probabilistic secret sharing algorithm and create key for focus point affirmation. The key sharing convention uses to process the diverse tree based key errand. Every last one of the focuses related with riddle information. The inside point's new key is using the riddle information as of now converse with each extraordinary focus points. The new key setup amidst correspondence orchestrate. The sender is honest to goodness if discovered MAC is the same as the got one. It utilizes lightweight cryptographic algorithm and obstruction against HELLO Flood Attack.

1.8.10. In Data Security:

In year 2014, Naitik Shah, Nisarg Desai and Viral Vashi[19] have presumed that cryptography give an answer for execute security structure, which depend on learning of characters and their blends, called keys, this blend is utilized to control unique information to some mixed content. Cryptography has turned into a cutting edge science with down to earth suggestions for protection, for expanding security of electronic information exchange. In this way, they give an answer for information security issue through cryptography method in view of ASCII esteem. To upgrade security of information exchange over web, they proposed another encryption procedure which utilizes ASCII estimation of character over which numerical figurings are finished. At that point with the utilization of Diffie Hellman, twofold code of controlled ASCII esteem are changed over in to dark code with utilization of key and finally cipher is changed over into Hex code and Transferred between clients.

1.8.11. In Recovering Secret Image:

In year 2011. John Blessuin, Rema, Jennifer Joselin[20] proposed another course of action in which a halftone picture HI is delivered utilizing the grayscale mystery picture GI by utilizing an error diffusion technique. A half-reviewed photo of the halftone pictures HI, called a halftone logo HL, is made by utilizing an interpolation headway. In this proposed conspire, the halftone logo HL is utilized to take in the unwavering idea of the changed grayscale mystery picture GI and the sensibility of the approach of amassed shadows.

There are five phases in this game plan:

1. Generation of Shares:

Shadows are made for mystery picture in the offer change step. In this development, apply the error diffusion technique to the grayscale picture GI to recover a halftone picture HI, the width and stature of HI are W and H. The halftone logo named HL, which is a half-instance of HI is made by utilizing the interpolation and error diffusion technique . In this development, the halftone logo HL is contracted to one-halftone picture HI in each estimation. Subjectively make two symmetric key K1 and K2. Encode pixels of HL with key K1 and symmetric cryptographic algorithm, for example, DES, when pixel are orchestrated at even segments of halftone picture HL, and after that scramble pixel of halftone picture HL with key K2 and symmetric cryptographic algorithm when pixel are masterminded at odd lines of halftone picture HL to derive the encoded halftone logo HL. By then make the offers utilizing picture packing interpolation technique and the key will be brought into the offers.

2. Self-Verifying Code Embedding

A half-attempted photo of the halftone picture HI , called a halftone logo HL, made by utilizing an interpolation technique is accentuated utilizing the guideline level repeat technique of the self-asserting Code Embedding. This technique influence a twofold self-check to code for each pixel and supplements the code over into the furthest right two bits of each pixel and therefore a halftone logo with self-affirmation points of confinement can be passed on.

3. Uncovering Phase

This section depicts in detail how to evacuate the halftone logo HL and the replicated mystery grayscale GI from the strategy of gathered shadows. By utilizing the reversible information masking design. The basic key K1 and the halfway shadow S1 are gotten from the shadow SH. Correspondingly, the second key K2 and the inside shadow 2 are gotten from the shadow SH2. By then package the essential direct shadow S1 into non-covering 7-pixel squares. By then augmentation every 7 pixel debilitate by a p (7,4) Hamming code in light of X squares isolated from 7*7 pixels in the halfway shadow S1, we get an arrangement of X hinders, with each square containing 3 bits. BY joining these X squares, copy the blended halftone logo. Interpret cleared encoded halftone picture HL by utilizing keys K1 and K2 for pixel organized in even lines and odd fragments in the blended halftone picture HL, independently. After the unwinding is done, the think halftone picture is acquired.

4. Avowing Phase

This stage asserts the unflinching idea of the repeated mystery picture and the game-plan of amassed shadows. The halftone picture HI, which is made from in the noteworthy stage, plays out the half-sampling by applying error diffusion and interpolation techniques to recover another halftone picture, called HI. In this stage, the halftone logo HL produced using the halftone picture HI is go over technique which conveys a twofold self-affirmation code for each pixel and slow the code once more into the furthest right valuable to no finish of each pixel, along these lines a halftone logo with self-check limits is formed.

5. Picture Recovering

   This stage recoups the copied mystery picture when the shadow is being bamboozled. The swindled picture is recuperated by applying Double-Sampling and pivot halftoning.

1.8.12. In WDM-Compatible DPSK Signal

In year 2013, Marcelo L.F. Abbade, Caulos A.Messani, Cleiton J.Alves, Guilherme M. Taniguti[21] investigate another wavelength division multiplexing perfect all optical cryptography technique that could be connected in TON. Such technique depends on the contemporary advances in the creation of optical band pass filters (OBPF) with limited bandwidth that permit single WDM signals to be partitioned in a few spectral slices. Optical encoding is then accomplished by giving diverse lessening and deferrals to each spectral side. The optical cryptography technique broke down in this work might be connected to TON spaces and is constituted by the optical signal handling step. A solitary WDM-perfect signal with fundamental optical bandwidth B 0 is part into n spectral slices. New all-optical cryptography technique, it depends on late advances in optical sifting and uses OBPF with slender bandwidth to slice bandwidth to slice WDM-good signal. After this, it uses a SAE organize took after by a SDE one. Our reenactment result propose that the technique give a decent execution to the encoded and in addition for the decoded signals which could be legitimately spread by separations higher than 300 km. The slice bandwidth is a key parameter for the accomplishment of the technique. The smaller such slices are, the more drawn out and more secure the cryptographic keys move toward becoming.

1.8.13. In Secure Information Management:

In year 2017, Lidia Ogiela and Marek R.Ogiela[22] propose another tradition that grants to guarantee information in different organization structures. The displayed information part procedures will concern cryptographic information part algorithms, and furthermore information sharing algorithms making use of psychological information investigation strategies. The insider perils methods will concern information generation methodologies and subjective information investigation techniques.Using the new approach, which relies upon psychological structures allow to guarantee the secured features and make the organization shapes more powerful. The game plan that cryptography started propels methodology for camouflaging information: coding it, scrambling it, guarding access to data.In the two information part and sharing algorithms, a mystery part holds one of n offers of the parceled information into which information I has been isolated. The period of separating information and flowing it among process individuals is therefore the same in the two information part and sharing algorithms. Information I is parceled between n process part. Everyone of them get one of n offers of the hole information, anyway this one offer alone is absolutely silly and mindless. Thusly, revealing a single area of the parcel information speaks to no peril to the security of the entire informational index. Trustees of the hole mystery store the information until the point that the moment that it ends up essential to mimic and reveal it. This for information part and sharing algorithms. Information part computation require uniting all n offers of the split mystery to copy the split information. If n-1 shares the joined information I won't process differs be imitated. Information sharing count require joining a particular number of offers m&lt;n, set at the period of portraying the computation to mimic information I. In this way, it is imperative to join only a picked number of mystery shares (m) to copy the information. The amount of mystery shares required to rehash information I depends upon what information sharing arrangement is picked. Courses of action of this compose are known as (m,n)- edge designs, where the number n connotes the amount of offers into which information I will be disconnected, however number m addresses the amount of offers totally required to duplicate information.

1.9 LATEST CRYPTOGRAPHIC TECHNIQUES:

As cryptography is all about hiding the information, so that it will be unreadable by the unauthorized parties. So, there are many techniques which helps us to achieve the goal of cryptography like DES, triple DES, AES, RSA, Blowfish, Twofish etc.

1.9.1 DES:

DES is a symmetric key block cipher which utilizes 16-round fiestal structure and has a block size of 64 bit and key length of 56 bit. In this, there are 16 indistinguishable phases of handling which are named as rounds. DES is by and large in view of the fiestal function.

Fiestal Function: It works on 32 bits at once and comprises of following four phases. To start with arrange is expansion in which the half block (32 bit) ventured into 48 bits with the assistance of expansion permutation by simply copying the half bits and the yield comprises of 48 bits. Second stage is Key Mixing in which the consequence of first stage is joined with the sub key with the assistance of XOR activity. For each round, the round-key generator produces the new key every one of 48 bits. Third stage is Substitution in which before handling by the substitution boxes or s-box, the block is divided into eight 6 bit blocks. The s-boxes give the center of the security of DES. Fourth stage is Permutation in which at last the 32 bit yield from the s-boxes are reworked by the settled permutation (p-boxes). The p-box is outlined such that the bit from the yield of s-box is spread crosswise over four diverse s-boxes in next round.

1.9.2 TRIPLE DES:

It is triple data encryption algorithm(also called TDEA or triple DEA). It is a symmetric key-block cipher which apply the DES algorithm three times on each data block. In triple DES, before using it, we generate a triple DES key say k which consists of 3 different DES keys k_1, k_2, k_3 which means the key length of 3TDES is 168 bits(3*56) and then distribute it. The encryption-decryption process in 3DES consists some steps. Firstly, Encrypt the plaintext in blocks by using single DES with key k_1. Then the output of the step 1 will be decrypted by using single DES with key k_2. Now, the output of the step 2 will be encrypted with key k_3 by using single DES. Then, the output of step 3 will be the cipher text. Now, decrypt the cipher text by just reversing the process.

1.9.3 AES:

AES remains for Advanced Encryption standard which is an asymmetric key block cipher having 128-bit information and key of 128,192, or 256-bit. It is particularly more grounded and speedier than the triple DES. AES plays out the entirety of its calculation on bytes as it regards 128 bit plaintext as 16 bytes plaintext and AES encodes utilizes 10 rounds for 128 bit keys, 12 rounds for 192-bit keys and 14-rounds for 256 bit key. For Encrypting, each round comprises of four sub forms: Byte Substitution, Shift rows, mix columns and include round key.

In Byte Substitution, the contribution of 16 input byte are substituted by gazing upward in a settled table which brings about the framework which comprises of four rows and four columns and afterward in Shift rows, each line of the lattice is shifted towards the left and is any section tumbles off out of the grid then it will embedded on the correct side of the line. Shifting is done according to a few standards like first line won't be shifted; Second column is shifted towards left by one position; third line is shifted towards left by two positions; fourth line is shifted towards left by three positions. At that point in mix Columns, every column of four bytes is changed utilizing a unique numerical capacity. This numerical capacity takes four bytes of one column as information and gives yield of four totally four bytes which essentially supplant the first one. The outcome is another new grid which comprise of 16 bytes. Last is Add Round Key in which, 16 bytes of the network are currently considered as 128 bits and XOR task is connected to the 128 bits of the round key.

For decryption , each round comprises same process as that of encryption process yet in invert arrange like first include round key at that point mix column at that point shift line and after that byte substitution.

1.9.4 RSA:

RSA algorithm is asymmetric algorithm because of its utilization of combine of keys. In this way, in this we have public key to encode our message and private key to unscramble it. The

Rivert-Shamir-Adleman(RSA) algorithm is a standout amongst the most secure public-key encryption technique. Be that as it may, this algorithm depends on the way that we don't have any effective any to factor vast number.

In Encryption-Decryption Process, assume, we have an encryption key(e, n) and decryption key(d, n). Along these lines, in this procedure, speak to any whole number between 0 to (n-1) as message. The extensive number can be broken into number of blocks. Be that as it may, each block will be spoken to by a whole number in a similar range. At that point, encode the message by raising it to the eth control modulo n. The outcome that turns out will be the ciphertext C. Presently, to unscramble that cipher content C, raise it to the power d modulo n. To decide the estimation of e, d and n. For that, we have a few tenets which are as per the following-

Pick any two vast prime numbers and signify these number as p and q. Presently $n= (p*q)$ where n is public. Presently process $\Phi (n)= (p-1) (q-1)$.Then select e with the end goal that $e< \Phi (n)$ and $gcd(e, \Phi (n))=1$. Presently <e, n> will be the public key. At that point find $d= e-1 \bmod \Phi (n)$. Presently <d, n> will be the public key. At that point $c=pe \bmod n$ and $P=cd \bmod n$ and recollect $p<n$.

1.9.5 BLOWFISH:

Blowfish is a symmetric encryption algorithm which contains 64-bit block cipher. This cryptographic algorithm is concocted by Bruce Schneier in 1993. At first, it is advanced for 32-bit processors with huge information stores. This cryptographic procedure is essentially quicker on a Pentium or PowerPC-class machine as contrast with the DES. Key lengths in blowfish cryptographic system may differ from 32 to 448 bits. Blowfish procedure is accessible uninhibitedly and planned as a substitute for DES or IDEA and it is utilized as a part of extensive number of items.

Blowfish algorithm is composed in thought with (i).Fast: It encrypts information on huge 32-bit microchips at a rate of 26 clock cycles for every byte. (ii) Compact: It can keep running in under 5K of memory. (iii) Simple: It utilizes addition, XOR, query table with 32-bit operands. (iv) Secure: The key length is variable, it can be in the scope of 32~448 bits: default 128 bits key length.

This algorithm is divided into two segments: Key-expansion and Data Encryption. Blowfish uses tremendous number of sub keys .So, in key expansion; it changes over a key at most 448 bits into a couple of sub key clusters with a total 4168 bytes. In data encryption, It is having an ability to rehash 16 times of framework. Each round contains key-subordinate stage and a key and data subordinate substitution. All are XOR activity and expansion task on 32-bit words. Simply extra tasks are four arranged exhibit data inquiry tables for each round.

1.9.6 TWOFISH:

Twofish algorithm is a symmetric block cipher. In Twofish algorithm, a single key is utilized for both encryption and decryption. Twofish algorithm contains a block if measure 128 bits and can acknowledge a key of any length up to 256 bits. Twofish algorithm is demonstrated quick on both 32-bit and 8-bit CPUs and furthermore in equipment. The blowfish algorithm is more adaptable as contrast with other cryptographic procedures. It can likewise be utilized as a part of system applications where keys are changed regularly and also in applications where there is almost no RAM and ROM accessible.

Twofish is a Feistel network which implies that in its each round, half of the content block is sent by means of a F capacity, and afterward the XOR operation is connected on the other portion of the content block. In each round of Twofish, two 32-bit words fill in as a contribution to the F work. In this, each word is partitioned into four bytes. Those four bytes are sent by means of four distinctive key-subordinate S-boxes. The four yield bytes are joined with the assistance of a MDS i.e., Maximum Distance Separable matrix and after that consolidated into a 32-bit word. At that point the two 32-bit words are consolidated utilizing a Pseudo-Hadamard Transform (PHT)[28], added to two round sub keys, at that point XOR with the correct portion of the content. There are additionally two 1-bit turns going on, one preceding and one after the XOR. Twofish likewise has something many refer to as "prewhitening" and "postwhitening;" additional sub keys are XORed into the content block both before the first round and after the last round.

1.9.7 CAESAR CIPHER:

The Caesar Cipher technique is one of the most punctual and least complex strategy for encryption technique. It's basically a kind of substitution figure, i.e., each letter of a given content is supplanted by a letter some settled number of positions down the letters in order. For instance with a move of 1, A future supplanted by B, B would progress toward becoming C, etc.

Encryption and decryption of a letter by a move n can be portrayed scientifically as $E_n(x)=(x+n) \bmod 26$

$D_n(x)=(x-n) \bmod 26$ respectively.

1.9.8 SERPENT:

Serpent is a symmetric block figure that has a place with a class of substitution-permutation systems. It was produced by Ross Anderson , Eli Biham and Lars Knudsen . In the form that was submitted for AES challenge the technique works on 128 bit blocks of information utilizing as a part of the procedures a 256 bit external key[24]. The change stream is separated into 32 uniform rounds rehashed over the information block with each round comprising of grouping of rudimentary activities. Each round requires its exceptional 128-bit round key; since the last round necessities two keys, aggregate of 33 distinctive round keys are required and these are created from the external key in a different key schedule[25].

1.9.9 International Data Encryption Algorithm (IDEA)

IDEA is a symmetric key block cipher. It utilizes a block cipher with a 128 bit key and is for the most part thought to be essentially secure. In this, 64-bit plaintext block is distributed four 16-bit sub-blocks, since all the logarithmic exercises used as a piece of the encryption procedure work on 16-bit numbers. Another procedure produces for each one of the encryption rounds, six 16-bit key sub-blocks from the 128-bit key[26]. Since a further four 16-bit key-sub-blocks are required for the subsequent yield transformation, a whole of 52 (= 8 x 6 + 4) various 16-bit sub-blocks must be delivered from the 128-bit key. The 52 16-bit key sub-blocks which are made from the 128-bit key are conveyed as takes after: First, the 128-bit enter is allocated eight 16-bit sub-blocks which are then particularly used as the underlying eight key sub-blocks.The 128-bit key is then reliably moved to the other side by 25 positions, after which the ensuing 128-bit block is again apportioned into eight 16-bit sub-blocks to be straightforwardly used as the accompanying eight key sub-blocks. The cyclic move system portrayed above is repeated until most of the required 52 16-bit key sub-blocks have been created.In Encryption process, In the essential encryption round, the underlying four 16-bit key sub-blocks are joined with two of the 16-bit plaintext blocks using expansion modulo 216, and with the other two plaintext blocks using enlargement modulo 216 + 1. The results are then prepared, whereby two more 16-bit key sub-blocks enter the estimation and the third logarithmic social event operator, the bit-by-bit specific OR, is used. At the complete of the key encryption cycle four 16-bit regards are made which are used as commitment to the second encryption round in a not entirely changed order. The procedure portrayed above for cycle one is reiterated in each one of the resulting 7 encryption rounds using particular 16-bit key sub-blocks for each blend. In the midst of the ensuing yield transformation, the four 16-bit regards conveyed toward the complete of the eighth encryption round are joined with the last four of the 52 key sub-blocks using expansion modulo 216 and increment modulo 216 + 1 to form the resulting four 16-bit cipher text blocks.

1.9.10 DNA CRYPTOGRAPHY

DNA cryptography is another field in cryptography which emerged with the advance of DNA computing. 1n 1994, Leonard Max Adleman has proposed this technique to give better information security. The principle motivation to acquaint this technique was with take care of issues that are either require tremendous measure of calculation or unsolvable by regular PC[3]. In DNA cryptography, each letter of the letters in order is changed over into various mixes of four bases i.e. a(adenine), T(thymine), g(guanine) and c(cytosine) such that it makes up the deoxyribonucleic Acid.

TABLE 1(a)

PARAMETERS	AES	TRIPLE DES	DES	RSA
DEVELOPER	Vincent Rijmen and Joan Daeman in Blegium NIST		IBM	Rivest, Adi Shamir and Leonard adleman
YEAR	2000	1998	1977	1977
KEY SIZE	128, 192 or 256 bits	112 bits or 168 bits	56 bits	>1024 bits
BLOCK SIZE	128,192 or 256 bits	64 bits	64 bits	Depends on key size
CIPHER TYPE	Rijndeal cipher	Symmetric key block cipher	Block cipher	Block cipher
NETWORK TYPE	Fiestal Network		Fiestal cipher	Common network
SECURITY ATTACKS	Chosen plain attack	Brute force attacks	Brute force attack	Timing attack
ADVANTAGES	It utilizes higher length key sizes, for example, 128, 192 and 256 bits for encryption. Subsequently it makes AES	Triple DES is easy to implement and accelerate in both hardware	Encryption and decryption takes the same algorithm so the function need to be reversed and the key should be	RSA is rather complex and it is almost impossible to decrypt the message without a private key.

	algorithm more hearty against hacking.		taken in opposite order.	
DISADVANTAGES	Hard to implement with software.	When the file or hard drive crash, it's hard to recover	Two chosen input to an S-box can create the same output.	RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer

TABLE 1(b)

PARAMETER	BLOWFISH	TWOFISH	SERPENT	IDEA
DEVELOPER	Bruce Schneier	Bruce Schneier counterpane system	Ross Anderson, Eli Biham, Lars Knudser	James Masser of ETH Zurich and Xuejia Lai
YEAR	1998	1998	1985	1991
KEY SIZE	32 to 448 bits	Upto 256 bits	256 bit	128 bits
BLOCK SIZE	64 bits	128 bits	128 bit	64 bits
CIPHER TYPE	Symmetric Block cipher	Clock cipher	Symmetric Block cipher	Block cipher
NETWORK TYPE	Fiestal Network	Fiestal Network	Substitution-permutation Network	Fiestal Network
SECURITY ATTACKS	Boomerang attack	Boomerang attck	Eaves Dropping	Narrow Bicliques attack
ADVANTAGES	Blowfish isn't liable to any licenses and is in this manner unreservedly accessible for anybody to	It enables implementers to tweak encryption speed, key setup time and code size to	It's the speediest algorithm in equipment, and the second quickest in programming	IDEA has been ended up being effective against numerous

	utilize.	adjust execution.	on the IA-64 design	cipher attack strategies.
DISADVANTAGES	Each match of clients needs a one of a kind, so as number of clients increment, key management ends up confused.	execution weren't useful for all employments.	execution weren't useful for all employments.	huge quantities of weak keys were found in IDEA[23]

CHAPTER 2

LITERATURE REVIEW

2.1 DNA

Deoxyribonucleic acid (DNA) is a chain of molecule that holds the instruction which is needed by an organism to develop, live and reproduce. DNA passed from parents to children and can be found inside every cell. DNA is made up of molecules which are called nucleotides and each nucleotide contains three components, sugar group, Nitrogen Base, Phosphate group. The nitrogen bases are of four types: Thymine (T), Guanine (G), Adenine (A), and Cytosine(C). So, the DNA's instruction and genetic code is determined by the order of nucleotides.

Nucleotides are joined together to form a spiral that creates a structure called double Helix as shown in figure 2. The structure of double Helix is same as like as ladder where the sides would be of phosphate and sugar molecules and bases would be the rungs. The base of one strand combines with the base of another strand like Adenine pair up with Thymine and Guanine pair up with Cytosine[27].

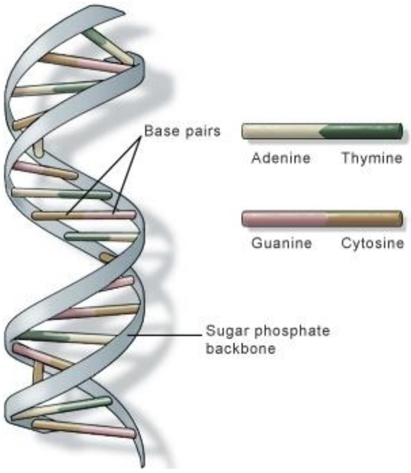

Figure 2.1 Double Helical Structure of DNA

2.2 DNA CRYPTOGRAPHY:

In 1994, Leonard Max Adleman has introduced a new technique to provide better data security called DNA cryptography. DNA cryptography provides data security, data confidentiality and data integrity which are the main aim of cryptography and provides more security as compare to other cryptographic techniques but it also takes more time complexity as compare to other cryptographic techniques for encryption and decryption. The DNA in this technique is utilized as a data transporter and the modern biological devices are utilized for execution[9].

In DNA cryptography, each letter of the alphabet is converted into different combinations of four bases in such a way that it makes up the deoxyribonucleic Acid.

DNA BASED CODING

DATA BASE	A	C	G	T
CODE	00	01	10	11

Table 2

In 2003, Jie Chen[2] introduced the DNA cryptographic approach in light of molecular theory, one-time pad and performed encryption and decryption of 2-D image. In 2004, Ashish Gehani et al. established the framework of DNA cryptography by utilizing molecular approach and the idea of one time pad which has official mystery, as indicated by Verman's and Shannon: creator of one time pad. They have proposed a technique for encryption and decryption which depends on DNA chip and one time pad. Along these lines, it is hard for the adversary to figure the encrypted message.

In 2005, Kazuo Tanaka[4] et al. proposed the DNA cryptographic approach in view of Public key. In this approach they have unmistakably clarified about the arrangement of public keys by utilizing solid supports mixture for PKA and ODN mixture for PKB. Subsequent to producing the keys, message is encoded in a DNA sequence with the assistance of one of the public key, which is additionally combined with the DNA synthesizer and after that encoded message sequence is legated with another public key. Presently the result of the past procedure is sent to the immobilization procedure and after that for PCR amplification, where the amplification is finished with the assistance of secret sequence, keeping in mind the end goal to decipher the encoded DNA sequence.

In 2006, Sherif T. Amin et al.[5] proposed the DNA cryptographic approach in light of symmetric key, where sequences are gotten from the genetic database and stay same at the two finishes i.e. sender and collector. Message is first changed over into binary format and after that to DNA format utilizing substitution. Once the substitution has been performed and message is as DNA sequence, at that point we pick the quadruple from the sequence we have gotten and mach it with the key sequence and where mach happens we take note of the position. Like this all the irregular position for each character in the plaintext are acquired and the document which contains these positions are our cipher text which is sent to the collector and after that decryption is perform backward request.

In 2011, Deepak Kumar and Shailendra Singh[6] proposed another secret data writing techniques in light of DNA sequences. They have clarified this calculation by utilizing a basic case of "HELLO" as a plaintext and create a ssDNA one time pad key of350 bits which is 70 times longer than the plaintext and perform encoding and decoding on the plaintext using symmetric key cryptography. Along these lines, to locate the correct key, foe needs to look among 4310 changed ssDNA strings which is relatively unimaginable.

In 2012, Sabari Pramanik and Sanjit Kumar Setua[7] proposed a new parallel DNA cryptography technique utilizing DNA modecular structure and hybridization technique which absolutely limit the time necessity. They have clarified how message is trading securely amongst sender and recipient with a case.

In 2012, Yunpeng Zhang[8] proposed a DNA cryptography in light of DNA piece assembly. In their calculation they have obviously specified how sender changes over the plaintext into binary sequence and afterward into long chain of DNA, which is additionally divided into little DNA chains. Key of short chains implantation happens in the parts and forward to the recipient as a cipher text and afterward beneficiary deciphers it and begins section reassembly to acquire the plaintext.

2.3 DATA HIDING SCHEME:

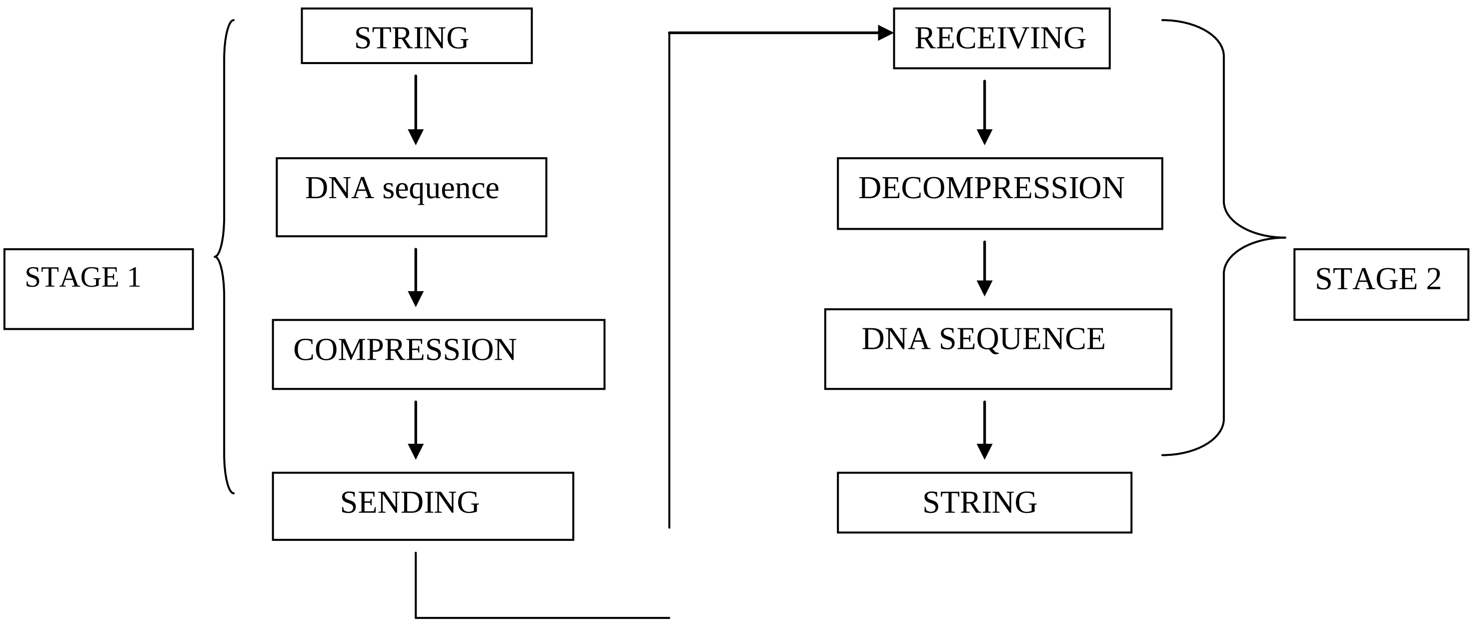

Figure 2.2 Flow diagram of Data Hiding Scheme

DNA SEQUENCE COMPRESSION:

The primary point of DNA compression is sparing time and space. Since, DNA sequence is built from four letters a, g, t and c which remains for adenine, guanine, thymine and cytosine separately and these sequences for the most part have rehashes. Since, DNA sequence contain just four bases that can be put away by utilizing two bits for each info image and that is the reason the standard compression apparatus neglects to do this as they utilize in excess of two bits for single information image. For DNA encoding, we have three techniques, two-bit encoding strategy, exact matching technique and estimated matching strategy. For encoding the DNA sequence, while handling the DNA string from left to right, recognize the exact number of rehashes or palindrome that gives the past occasions in the effectively prepared content and afterward encode then by the length and position of a prior event.In two bit encoding method, each character can be easily encode using two bits i.e., 00 for a, 01 for c, 10 for g and 11 for t.

In Exact pattern matching, this algorithm will find that whether the likelihood will prompt effective inquiry or unsuccessful pursuit. The issue can be expressed as: Given a pattern p of length m and a Text T of length n (m ≤ n). Discover every one of the events of p in T. The matching should be exact, which implies that the exact word or pattern is found. Some exact string matching algorithms are Naïve Brute force algorithm, Boyer-Moore algorithm , KMP Algorithm.

In inexact matching, issue by and large can be expressed as: Given a pattern P of length m and content T of length n (m ≤ n). Discover every one of the events of sub string X in T that are like P, permitting a predetermined number, say k diverse characters in comparative matches. The Edit/change tasks are inclusion, cancellation and substitution. Vague/Approximate string matching algorithms are ordered into: Dynamic programming approach, Automata approach, Bit-parallelism approach, Filtering and Automation Algorithms. Inaccurate arrangement information emerges in different fields and applications, for example, computational science, sign al handling and content preparing. Pattern matching algorithms have two primary destinations:

(i)Reduce the quantity of character examinations required in the worst and average case investigation.

(ii) Reducing the time prerequisite in the worst and average case investigation.

CHAPTER 3

PROPOSED WORK

3.1 PROPOSED WORK

In proposed work, various different cryptographic algorithms like two bit encoding algorithm, exact matching, approximate matching, DES, triple DES, AES, RSA, Blowfish, Twofish, Caesar cipher, Serpent, IDEA are implemented with different strings having different patterns. Patterns like string in which every letter is occurring once, string with every letter is occurring twice, whole string is repeating two times, whole string is repeating three times, palindrome string, string with different length. These strings has been taken as an input and then their encoded form has been compared.

CHAPTER 4

RESULTS AND EXPERIMENTAL ANALYSIS

In this chapter, the proposed work is developed in Dev C++ IDE using Intel core i3 processor, 2GB RAM. In this work, different cryptographic algorithms like two bit encoding algorithm, exact matching, approximate matching, DES, triple DES, AES, RSA, Blowfish, Twofish, Caesar cipher, Serpent, IDEA are implemented with different strings. Strings with different patterns like string in which every letter is occurring once, string with every letter is occurring twice, whole string is repeating two times, whole string is repeating three times, palindrome string, string with different length has been taken as an input and then their encoded form has been compared.

TABLE 3(a)

STRING	atcg	aattccgg	aaatttcccggg	Atcgatcg	Atcgatcgatcg	Atg	Atgatg
FEATURE	Every letter is occuring once.	Every letter is occuring two times	Each letter is occurring three times	String is repeating two times	String is repeating three times	String length is three.	String length is six
Two bit encoding	00110110	0000111101011010	000000111111010101101010	0011011000110110	001101100011011000110110	001110	001110001110
Exact matching	000011	000011100100	000011100100000100	000011100100	000011100100000100	000011	000011100010
Approximate matching	000010010011000	000011110011000	0000111100110000000100100111	000001110011000	0000111100110000000100100111	000001110011000	000011010011000
DES(key-plain ciphertexts)	U5JIPipptQo=	6rDyrOhzFEI=	oBVfcNtOpqSu4FPEW+CsAA==	I6cSoVOEfQ4=	6cSoVOEfQ5Tkkg+Kmm1Cg==	ccfdBHEH7dY=	52oOG07GQpg=
Tripl	jpKSBsHU	JGFf3i/TYi	3ZNs5f+7g	v65PKLoz+	v65PKLoz+	v65PKLoz	NG5ivInZ

e DES(key-plain ciphertexts)	oK4=	k=	rnRQcZwNHPktA==	8Y=	8aOkpIGwdSgrg==	+8aOkpIGwdSgrg==	3Y0=
AES(key-plain ciphertexts)	FDDO2MT9nSKNyR9Yb5Wusg==	Gpa0NfNJUkM6J2ojXioxpw==	RGUm4IjA7Kh8S0t9nzTUFA==	fTR6AWFYNNwuiETu4Abqkg==	NMD7yd3209MV4CJE/dk7iQ==	UPdBiVxzIr4edp/jgvN/EA==	6Jb3dHIH27Q+cRyvm3/Aag==
RSA(prime numbers- 7 and 11)	aÑåâ	aaÑÑåååâ	aaaÑÑÑååååââ	aÑåâaÑåâ	aÑåâaÑåâaÑåâ	AÑâ	aÑâaÑâ
Caesar Cipher(shift by 4)	exgk	eexxggkk	Eeexxxgggkkk	exgkexgk	exgkexgkexgk	Exk	Exjexk
Blowfish(key-plain ciphertexts)	iuLLhk/oRU8=	vATfM5dgaXg=	xJNChjvjC5lH6/siWXQrSg==	GMOaAGHlDtI=	GMOaAGHlDtKK4suGT+hFTw==	2QeEX/UhB7U=	rSH/GCEc34A=
Twofish(key-plain ciphertexts)	oiq2gYjRbiBRQDMsYOf0Zw==	zvCVrv1jJZur6jmMGpt3Qg==	Tl2QXTTDsag7/+L3ibMJRw==	gsd8WRTHDfoFByRFxD0QOQ==	4iIXzGnP00+mp84AhUt+PA==	Z7efeRIcGEt4LoXje1UcFQ==	JhiSIk0urdTrhc5uuAj/6w==
Serpent	RPdb9CcZDFa+pQonR5rjgA==	IFHAw6cp6YOObuqnL4Levg==	RAtE2rkyBLug+D2PYBBDZg==	chbKPJzjXbPnNk6pfdOsxA==	3GpHH7cbHS9bGp9ysj8QMQ==	UkD/qs8DK7Xdqj9tSAhOWQ==	nw7Cv1ZHlrhChPjXwuB1Ig==
IDEA(key-plain ciphertexts)	JARjmYghcNA=	L+OqFbD9VKD/SntOnekHFw==	V3fMUKf5onfvZGztGcWHEg==	8sHHXfcwJsj/SntOnekHFw==	8sHHXfcwJsgkBGOZiCFw0A==	9po68ZUSj3I=	j97fooQaUpk=

Table 3(b)

STR	atgatgatg	atgta	atgcgta	atgccgta	aaa	Aaaa	Aaaaa

ING							
FEATURE	String length is nine	Palindrome string with length five	Palindrome string with length six	Palindrome string with length seven	Same letters with string length three	Same letters with string length Four	Same letters with string length five
Two bit encoding	001110001110001110	0011101100	00111001101100	0010110101101100	000000	00000000	000000000
Exact matching	000011100100000001	000011100001	000011100011	000011100100	000011	000011	000011100001
Approximate matching	0000111100110000000001100111	000010110011000	000011110011000	000011110011000	000001110011000	000010010011000	000010110011000
DES (key-plain ciphertexts)	4QQWWXkozq9BvA3I5Suvsw==	9ANdkKzfym4=	jwPWBHDzALQ=	QiJOvIMc7ik=	H23UKnZgawg=	sc9jAxhw91A=	p6RG1CL3z6k=
Triple DES (key-plain ciphertexts)	uOwdoV0Ad2IoiABRHg0uqg==	WbJgUjI9eTs=	PXLxCzOZTqU=	tw/yqaKdY+o=	kGVdbMc9wEI=	0iyLT8Flbws=	srzgwlKtu8k=
AES (key-plain ciphertexts)	2aHkisoZnXRwHzvXJ0IpOQ==	ekID0zmd1tgNPaP+8HZpsQ==	s0Uqr0xGM3l/TieQEnhEpQ==	JkTgletXf9wWksRCSWyMjA==	2O0076MXXvKEvqJf/nd8Qg==	YB8OCKerPeSVCJgn9cCY3Q==	t3Ov506yWVmDuerGLUJylw==
RSA (prime numbers-7 and 11)	aÑâaÑâaÑâ	AÑâÑa	aÑâåâÑa	aÑâååâÑa	aaa	Aaaa	aaaaa
Caesar Cipher(sh	exkexkexk	Exkxe	exkgkxe	Exkggkxe	Eee	Eeee	eeeee

ift by 4)							
Blowfish(key-plain ciphertexts)	Gh8lL8ITswstMYq7GuczPw==	FtRcGZlPXUs=	rwaxt8DCCps=	ClsUqXKAAPw=	JL5dYunpxbE=	k+syNpIzxdA=	un/1RIkoXWk=
Twofish(key-plain ciphertexts)	VmiSMdz13EVtWOnzNE1w3w==	p7rVtZS5ZAowhGKam2/STg==	i1U3tSSBkTdCmgTOS1ZrAg==	qE5S6tZx9Dt55XveqLA2cg==	LkNl6LCRPFpVeLqIxrGUww==	V8dvOO/UTv/qQPo/3UxypQ==	GCJLCXyWximIDS6tWUGYjw==
Serpent	SZ7b4lZhDi7tgeKP22s+9Q==	c0Miq0IVp1tyt9AwokEBcA==	4sYxlUFXmB/UtJS3u81XFw==	yRatTJ7F3IHGQH1pA/6kJQ==	R560j0ZK7Ul1pqh+99pGIA==	0EcI7TMePKnkog1xofShDw==	nXrMxX7puybclRbSJhWF8w==
IDEA(key-plain ciphertexts)	B8nySjgeVl09C95J1YsDmA==	0yx300YTP6s=	FXl9zg7kAOY=	7Z+WsoH3mdH/SntOnekHFw==	3WmJKTx2OBs=	hqq9RLYlFug=	gm8G73GxdCE=

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION

Cryptography is a technique which is used to secure the communication and to provide data confidentiality and data integrity. DNA cryptography is a technique which hides the data in terms of DNA sequence. This technique converts each alphabet of letter into a combination of four base i.e., Adenine, Thymine, Cytosine and Guanine that makes the human DNA. This paper has introduced a data hiding scheme which is based on DNA sequence technique This paper has given a description of four techniques two-bit encoding method, exact matching method and inexact matching method which has been used to compress the DNA sequence.

5.2 FUTURE SCOPE

DNA cryptography is a promising field for doing examination and some quantum of commitments can be made to the accompanying:

- Looking into the integrity factor of the algorithm.
- Can be reached out for steganography, to give more layer of security.
- Improving space complexity of this algorithm.

REFERNCE

1. Kumar, Deepak, and Shailendra Singh. "Secret data writing using DNA sequences." In *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on*, pp. 402-405. IEEE, 2011.
2. Chen, Jie. "A DNA-based, biomolecular cryptography design." In *Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on*, vol. 3, pp. III-III. IEEE, 2003.
3. Pramanik, Sabari, and Sanjit Kumar Setua. "DNA cryptography." In *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on*, pp. 551-554. IEEE, 2012.
4. Tanaka, Kazuo, Akimitsu Okamoto, and Isao Saito. "Public-key system using DNA as a one-way function for key distribution." *Biosystems* 81, no. 1 (2005): 25-29.
5. Amin, Sherif T., Magdy Saeb, and Salah El-Gindi. "A DNA-based implementation of YAEA encryption algorithm." In *Computational Intelligence*, pp. 120-125. 2006.
6. Kumar, Deepak, and Shailendra Singh. "Secret data writing using DNA sequences." In *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on*, pp. 402-405. IEEE, 2011.
7. Pramanik, Sabari, and Sanjit Kumar Setua. "DNA cryptography." In *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on*, pp. 551-554. IEEE, 2012.
8. Zhang, Yunpeng, Bochen Fu, and Xianwei Zhang. "DNA cryptography based on DNA Fragment assembly." In *Information science and digital content technology (ICIDT), 2012 8th international conference on*, vol. 1, pp. 179-182. IEEE, 2012.
9. Pramanik, Sabari, and Sanjit Kumar Setua. "DNA cryptography." In *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on*, pp. 551-554. IEEE, 2012.
10. Mathur, Raghav, Shruti Agarwal, and Vishnu Sharma. "Solving security issues in mobile computing using cryptography techniques—A Survey." In Computing, Communication

& Automation (ICCCA), 2015 International Conference on, pp. 492-497. IEEE, 2015.

11. Bukhari, Sadaf, Muhammad Shoaib Arif, M. R. Anjum, and Samia Dilbar. "Enhancing security of images by Steganography and Cryptography techniques." In Innovative Computing Technology (INTECH), 2016 Sixth International Conference on, pp. 531-534. IEEE, 2016.
12. Daisy, V. Annie, C. Vijesh Joe, and S. Shinly Swarna Sugi. "An image based authentication technique using visual cryptography scheme." In Inventive Systems and Control (ICISC), 2017 International Conference on, pp. 1-6. IEEE, 2017.
13. Knežević, Karlo. "Combinatorial Optimization in Cryptography." In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on, pp. 1324-1330. IEEE, 2017.
14. Patel, Trupti, and Rohit Srivastava. "A new technique for color share generation using visual cryptography." In Inventive Computation Technologies (ICICT), International Conference on, vol. 2, pp. 1-4. IEEE, 2016.
15. Das, Ria, and Indrajit Das. "Secure data transfer in IoT environment: adopting both cryptography and steganography techniques." In Research in Computational Intelligence and Communication Networks (ICRCICN), 2016 Second International Conference on, pp. 296-301. IEEE, 2016.
16. Kester, Quist-Aphetsi, Laurent Nana, Anca Christine Pascu, Sophie Gire, Jojo Moses Eghan, and Nii Narku Quaynor. "Feature based encryption technique for securing forensic biometric image data using AES and visual cryptography." In Artificial Intelligence, Modelling and Simulation (AIMS), 2014 2nd International Conference on, pp. 199-204. IEEE, 2014.
17. Mateescu, Georgiana, and Marius Vladescu. "A hybrid approach of system security for small and medium enterprises: Combining different cryptography techniques." In Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on, pp. 659-662. IEEE, 2013.
18. Selvam, R., and A. Senthilkumar. "Cryptography based secure multipath routing protocols in wireless sensor network: a survey." In Electronics and Communication Systems (ICECS), 2014 International Conference on, pp. 1-5. IEEE, 2014.
19. Shah, Naitik, Nisarg Desai, and Viral Vashi. "Efficient Cryptography for data security." In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on, pp. 908-910. IEEE, 2014.
20. Blesswin, John, and Jenifer Joselin. "Recovering secret image in Visual Cryptography."

In Communications and Signal Processing (ICCSP), 2011 International Conference on, pp. 538-542. IEEE, 2011.

21. Abbade, Marcelo LF, Carlos A. Messani, Cleiton J. Alves, Guilherme M. Taniguti, Iguatemi E. Fonseca, and Eric AM Fagotto. "A new all-optical cryptography technique applied to WDM-compatible DPSK signals." In Transparent Optical Networks (ICTON), 2013 15th International Conference on, pp. 1-5. IEEE, 2013.
22. Ogiela, Lidia, and Marek R. Ogiela. "Insider threats and cryptographic techniques in secure information management." IEEE Systems Journal 11, no. 2 (2017): 405-414.
23. Singh, Harivans Pratap, Shweta Verma, and Shailendra Mishra. "Secure-International Data Encryption Algorithm." *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering* 2, no. 2 (2013): 780-792.
24. Aghajanzadeh, Naser, Fatemeh Aghajanzadeh, and Hamid Reza Kargar. "Developing a new hybrid cipher using AES, RC4 and SERPENT for encryption and Decryption." *International Journal of Computer Applications* 69, no. 8 (2013).
25. Anderson, Ross J., Eli Biham, and Lars R. Knudsen. "The Case for Serpent." In *AES Candidate Conference*, pp. 349-354. 2000.
26. Chang, How-Shen. "International data encryption algorithm." *jmu. edu, googleusercontent. com, Fall* (2004).
27. Pramanik, Sabari, and Sanjit Kumar Setua. "DNA cryptography." In *Electrical & Computer Engineering (ICECE), 2012 7th International Conference on*, pp. 551-554. IEEE, 2012.
28. Aparna, K., J. Solomon, M. Harini, and V. Indhumathi. "A Study of Twofish Algorithm." *International Journal for Engineering Research and Application (IJERA), 4 (2)* (2016): 148-150.