Secure Transfer Of Data In Cloud Computing Using DNA Cryptography With Cipher Techniques

Posted on March 12, 2025

Abstract

Cloud computing is a type of distributed computing that allows organizations to store and access data on-demand. It is commonly used for various applications such as network services, storage, and platform services. However, many organizations are not excited about using it due to security concerns.

Various researchers have been developing various methods to improve the security of cloud computing. One of these is the Bi-directional DNA encryption algorithm. However, this method only focuses on the character set, ignoring the non-English users.

When it comes to storing data in the cloud, it is important that the files are encrypted along with the name of the file. This ensures that the data is secure when it is transferred to other companies or vendors.

Introduction

The rise of cloud computing has created a major opportunity for IT professionals. This paper aims to provide a comprehensive review of the various technical issues that face the implementation of cloud computing. There are two types of cloud computing: public cloud and private cloud. Public cloud refers to the use of a pay-per-use model. On the other hand, the private cloud is a distributed model. In hybrid cloud computing, the various computing services are consumed by both the public and private cloud services. Software as a Service, or SaaS, is a type of cloud computing that allows customers to run a single service on a single cloud. A platform as a service, or PaaS, is a type of cloud computing that allows organizations to create and maintain their applications. It is additionally known as Infrastructure as a Service or IaaS. This type of cloud computing provides various services, such as storage, network capacity, and data centres.

Literature Survey

The security of data stored in cloud computing is a major concern. Various methods are used to

protect data in cloud computing. These include encryption, digital signature, and message authentication. In this article, we will talk about some of the common security problems that cloud computing can face.

Deoxyribonucleic Acid Based Nonce-Misuse-Resistant Authenticated Encryption Algorithm [1]

Mr. Harichandana Akumalla and Mr Ganapathi Hegde[1]. The paper presents a new algorithm that is designed to improve the efficiency and security of cloud computing by implementing a nonce-misuse-resistance algorithm. This method is based on the DNA block's critical property, allowing it to secure the key. In order to perform this computation, the block's processing unit uses the data structure of the ASCII code table to convert the input key into its equivalent base formats. Due to the increasing number of public channels for exchanging keys, the need for a secure method to exchange them has become more prevalent. This paper presents a new algorithm that is based on the DNA block's critical property. It is compared with the AES-GCM standard. Here, we see that content is encrypted inside the file but not along with the file name. AES-GCM, the attacker can easily change it to anything he wants, and GCM will never notice.

Union of RSA algorithm, Digital Signature and Kerberos in Cloud Security [2]

Mr. Mehdi Hojabri and Mr. Mona Heidari [2]. The goal of this paper is to perform a study on the concept of authentication services using the authenticated server, which is a part of the framework known as KRB. After validating the users, the server creates the session key and the ticket-granting ticket. The users then send the ticket and the session key to the ticket-granting server.

After validating the users, the server sends the ticket and the session key to the ticket-granting server. The users then send the request service to the cloud service provider to use the services. After doing this, the user can access the cloud. For better security, the service provider uses a combination of encryption and decryption algorithms. They also use a digital signature for authentication. Here, we see that content is encrypted inside the file but not along with the file name. It is easy for hackers to predict the file name and guess the content of the file even though it is encrypted.

Hiding Information in the DNA Sequence Using DNA Steganographic Algorithms with Double-Layered Security

[3]

Vinodhini R. E. and Malathi P. [3]. The goal of this paper is to introduce three different algorithms that are used to protect sensitive data from unauthorized access. These are an insertion algorithm, an addition/distraction algorithm, and a substitution method. The algorithms are an RSA-based insertion algorithm, a complementary algorithm using the Addition/Subtraction rule, and a combination of insertion and substitution methods with XOR operation. For instance, if you have 8 bits of data that you want to encrypt, but you decided to XOR each of them against the results of a coin flip, then the only way to decrypt them is by someone with a good knowledge of the coin flip results. But as mentioned here in the above paper[2]. The problem arises with the file name. The first is to encrypt the actual data being stored so that you can't get that data (easily) without the key. However, in that case, you can still open the archive and view the file names (i.e., the directory hierarchy) within it. Only once you try to get the file content will you need the key.

If you don't even want people to see those file names without the key, you should encrypt those as well.

Implementation of a digital signature with an RSA encryption algorithm to enhance the data security of the cloud in cloud computing [4].

Uma Somani, Kanika Lakhani, and Manish Mundra [4] In this paper, we introduce two types of enterprises: one is an organization that has public data, and the other is a company that has a private cloud. The two methods that are used to secure communication are the Digital signature and the RSA algorithm. In this case, the former takes the data from the cloud, while the latter gives the B the secure data.

The first step in implementing the Digital signature is to create a message digest, which is a function that is used to crush the data or document into little pieces. After that, the two methods will perform a combination of encryption and decryption to secure the communication. With the help of the public key and the private key, A will encrypt the data, and B will decrypt it. But as mentioned here in the above paper[2]. The problem arises with the file name. The first is to encrypt the actual data being stored so that you can't get that data (easily) without the key. However, in that case, you can still open the archive and view the file names (i.e., the directory hierarchy) within it. Only once you try to get the file content will you need the key.

If you don't even want people to see those file names without the key, you should encrypt those as well.

Proposed Work

In the previous section, we discussed the various security problems that are encountered when using cloud computing. In this paper, we introduce bi-serial DNA, an encryption algorithm that provides two levels of security for file names and file content. It also adds one more level of encryption of the Cipher technique before the DNA process gets encrypted. This adds stronger security to the purpose of storing the data.

Various Cipher Technique

Substitution Cipher / Caesar Cipher: Encryption is a process that involves hiding some data. When plain text is used, it becomes hard to read and is referred to as ciphertext. In a substitution cypher, the character from the given set of characters is replaced by another set of characters with a key. For instance, if A shifts from one set of characters to another, then A becomes B, and so on.

Mathematical representation

The process is represented by a modular arithmetic scheme that allows one to transform letters into numbers. For instance, if A shifts from one set of characters to another, then A becomes B, and so on.

$$E_n(x) = (x + n) mod\ 26$$

Encryption phase with Shift n

$$D_n(x) = (x - n) mod\ 26$$

Decryption phase with Shift n

Keyword Cipher: A keyword cypher is a type of monoalphabetic substitution that allows one to determine the letter matchings of a given word to the plain alphabet. After the word is removed, the key is used to determine the corresponding letter matchings in the ciphertext. The rest of the letters are then used in an alphabetical order.

Encryption: The first line of the input contains the keyword that you wish to enter, while the second line contains the string that you have to encrypt.

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y

Encrypted: K R Y P T O S A B C D E F G H I J L M N Q U V W X

The keyword Kryptos is used to encrypt the message “knowledge is power.” All of the letters in the string are then converted into numbers.

Encrypting the message: Knowledge is Power.

Encoded message: IlmWjbaEb GQ NmWbp

Decryption: To decode the message, you check the position of the given message in encrypting text with the plain text.

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y

Encrypted: K R Y P T O S A B C D E F G H I J L M N Q U V W X

Message: PTYBIATLEP

Deciphered Text: DECIPHERED

Now, how do we generate the deciphered string? We search for ‘P’ in Encrypted Text, compare its position with a plain text letter, and generate that letter. So ‘P’ becomes ‘D’, ‘T’ becomes ‘E’, ‘Y’ becomes ‘C’, and so on.

DNA Digital Coding

In the field of information science, the digital coding is encoded by two states 0 and 1 and a combination of 0 and 1. However, in DNA, it can be encoded by four different bases. These are ADENINE, THYMINE, CYTOSINE, and GUANINE. There is a possibility of 4! =24 patterns by using the encoding format (0123/ATGC).[4][17]

Binary value	DNA digital coding
00	A
01	T
10	G
11	C

Table 1. DNA Digital Coding

Key Combination

In this example, we are using ATGC as a key. Each bit has two bits, which are known as A=00, T=01, and C=11. By using ATGC, we can generate various key combinations, which are given in Table 2. We can then send and receive a 72-bit key using the same algorithm. The key value is sent to the receiver side by means of a random exchange.[4][17]

KEY COMBINATION	PATTERNS	VALUES
AA	0101	5
AT	0011	3
AG	0001	1
AC	0010	2
TA	0110	6
TT	1111	15
TG	0111	7
TC	1001	9
GA	1010	10
GT	0100	4
GG	1000	8
GC	1100	12
CA	1110	14
CT	1011	11
CG	0000	0
CC	1101	13

Table 2: Key combination

3. A. Encryption Process

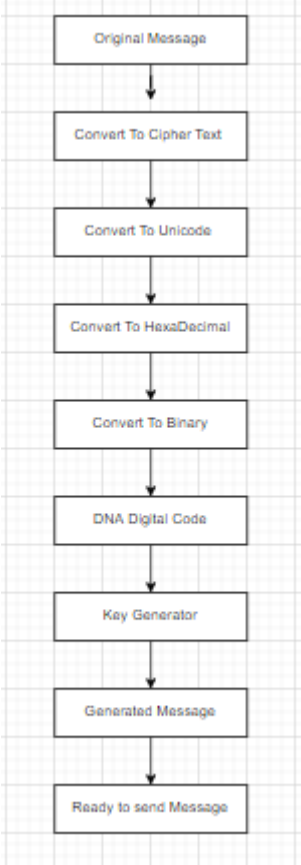

Fig 1: Encryption process

To understand the proposed workflow chart, we first need to consider an example. In this case, we are dealing with encryption operations for plain text “Testing”.

Here, we are using the “Keyword Cipher” to convert plain text. So, we get cipher text “ntmnbgs” this will be sent for DNA cryptography methods further. We are using multiple encryption methods to make the content structure strong and make it difficult for the hacker to hack the content.

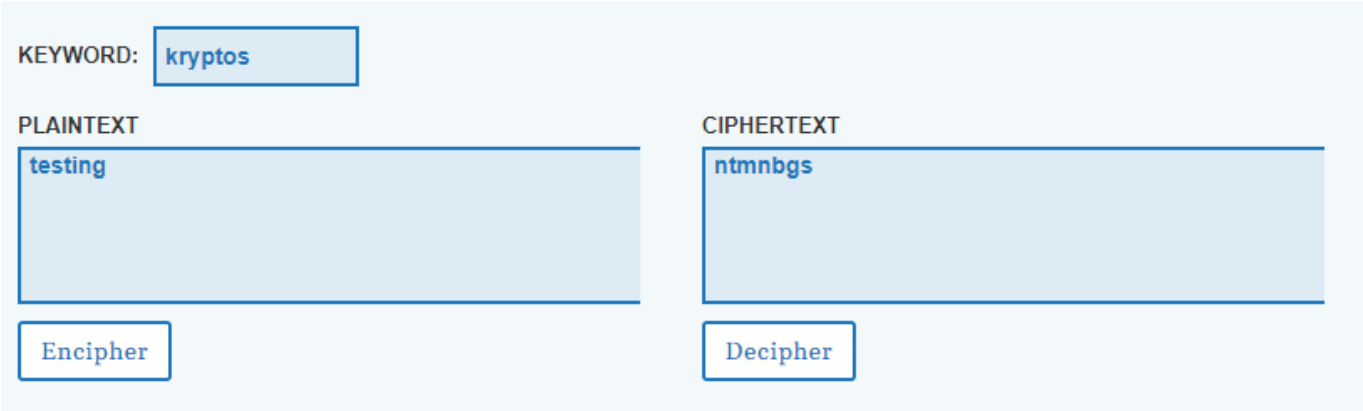

Fig 2: Keyword cipher conversion

Plain text: Testing

Cipher text: ntmnbgs

Unicode / ASCII: u006Eu0074u006Du006Eu0062u0073

Hexadecimal value:
5c75303036455c75303037345c75303036445c75303036455c75303036325c7530303733

Binary Value:

01011100011101010011000000110000001101100100010101011 1

00011101010011000000110000001101110011010001011100011101

01001100000011000000110110010001000101110001110101001

01100000011000000110110010001010101110001110101001

10000001100000011011000110010010111000111010100110 0

00001100000011011100110011

DNA Digital coding: From Table 1 w,e can write

TTCATCTTACAAACAAACTGTATTTTCATCTTACAAACAAACTCACT

ATTCATCTTACAAACAAACTGTATATTCATCTTACAAACAAACTGTAT

TTTCATCTTACAAACAAACTGACAGTTCATCTTACAAACAAACTCACAC

Now, from Table 2, the amplified message is generated; the amplified Message

1111111010011111001001010010010100100111011011111111111010011111 0010010

1001001010010100100100111011111111010011111100100101001001010010011101 10

0110111111101001111100100101001001010010011101101111111111010011111001

0010100100101001001110010000111111111010011111001001010010010100101001001 00010

3.B. Decryption Process

Now, at the receiver side, the receiver receives the amplified message and ATGC key for decryption.

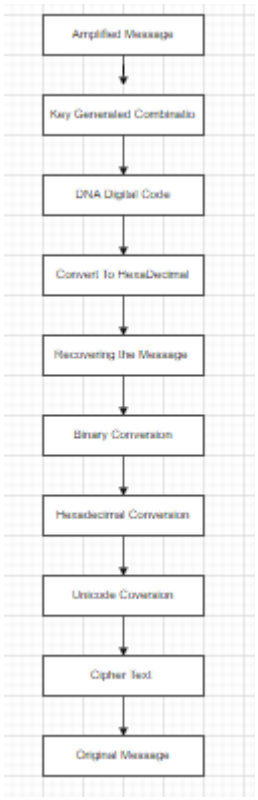

Fig 3: Decryption Process

Amplified message

1111111010011111001001010010010100100111011011111111111010011111

0010010100100101001010010010011011111110100111110010010100010

0101001001110110011011111110100111110010010100100101001001110

1101111111111101001111100100101001001010010011100100000111111111

0100111110010010100100101001010010010010

DNA Digital coding

TTCATCTTACAAACAAACTGTATTTTCATCTTACAAACAAACTCACTATTCA

TCTTACAAACAAACTGTATATTCATCTTACAAACAAACTGTATTTTCATCTT

ACAAACAAACTGACAGTTCATCTTACAAACAAACTCACAC

Binary Value:

01011100011101010011000000110000001101100100010101011100011110

10100110000001100000011011100110100010111000111010100110000000

11000000110110010001000101110001110101001100000011000000011011

00100010101011100011101010011000000110000001101100011001001O

11100011101010011000000110000001101110011001l

Hexadecimal value:
5c75303036455c75303037345c75303036445c75303036455c75303036325c7530303733

Unicode / ASCII: u006Eu0074u006Du006Eu0062u0073

Cipher text: ntmnbgs

Plain text: Testing

Conclusions

The main challenge of cloud usability is data security. Various types of algorithms, such as DNA encryption, D-Hellman, and Secure Sockets Layer, are available to provide secure access to the data stored on the cloud. BDEA is a two-layer security algorithm that is used to protect the character sets in ASCII text. In this paper, we propose a system that uses BDEA to implement two-layer security for the character sets for the content of the file and also the file names.

This paper aims to provide a framework that can be used by cloud users to improve the security of their data. In the future, we will study the various attacks that can be performed on the file contents and the file itself.

Acknowledgements

We authors would like to convey our sincere gratitude to Amrita School of Engineering, Bangalore, for providing a congenial working environment and constant support in completing our project.

Results / Snapshot


DNA CRYPTOGRAPHY IN CLOUD COMPUTING
Open the Source File :
testing.txt
Browse
APPLY DNA ALGO
File content
ntmnbs
Send Packets
Exit
Status Information
File Loaded
DNA Encoding Started
DNA Encoding Completed
Sending Packets to Destination
Packets Sent to Destination
DNA Encoding Started
Insider
MP
MP
MG
Destination
Internet
Source
MAP
STA
MAP

Fig 4: Source

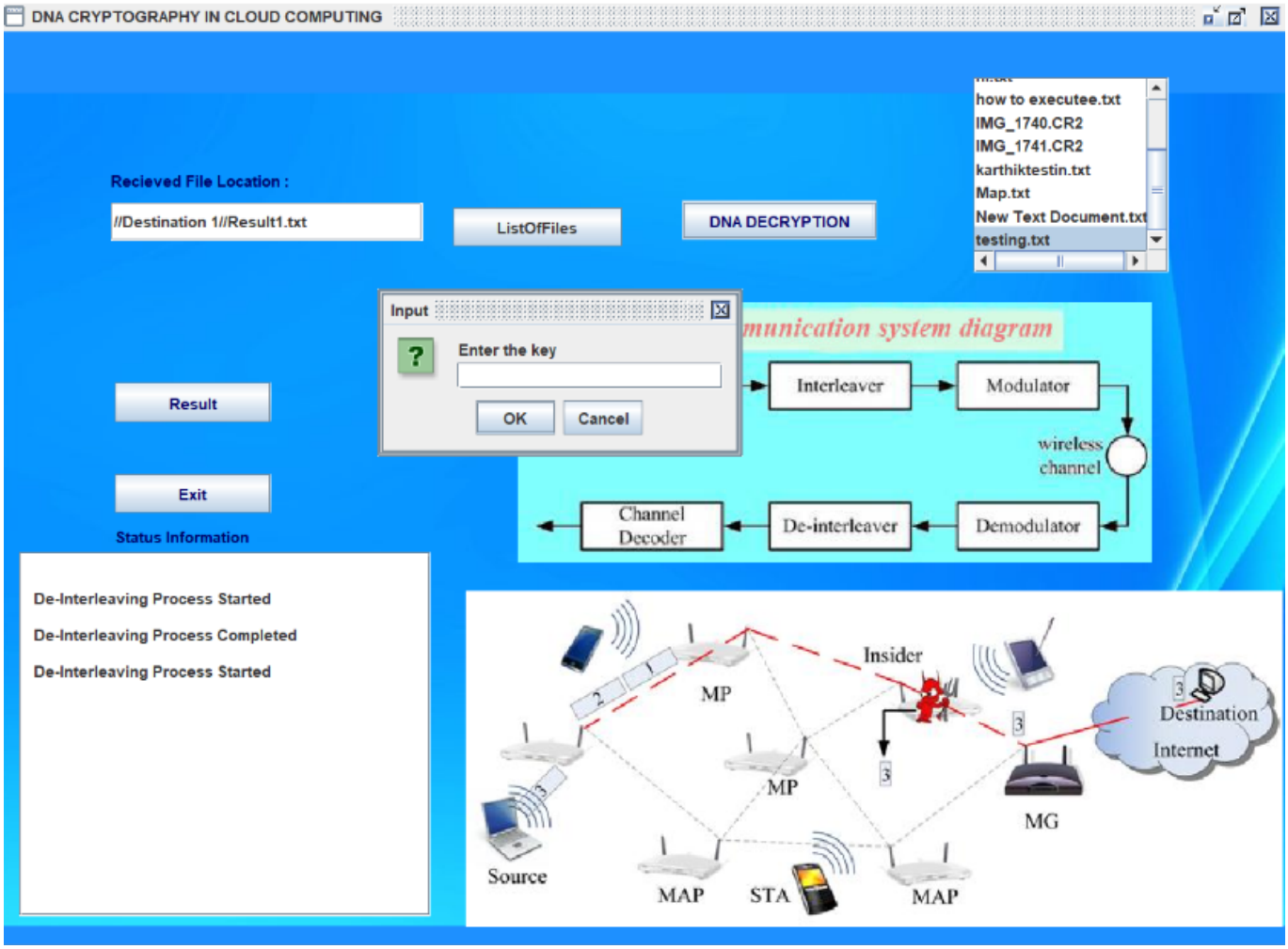

Fig 5:Decryption Process with the key needed

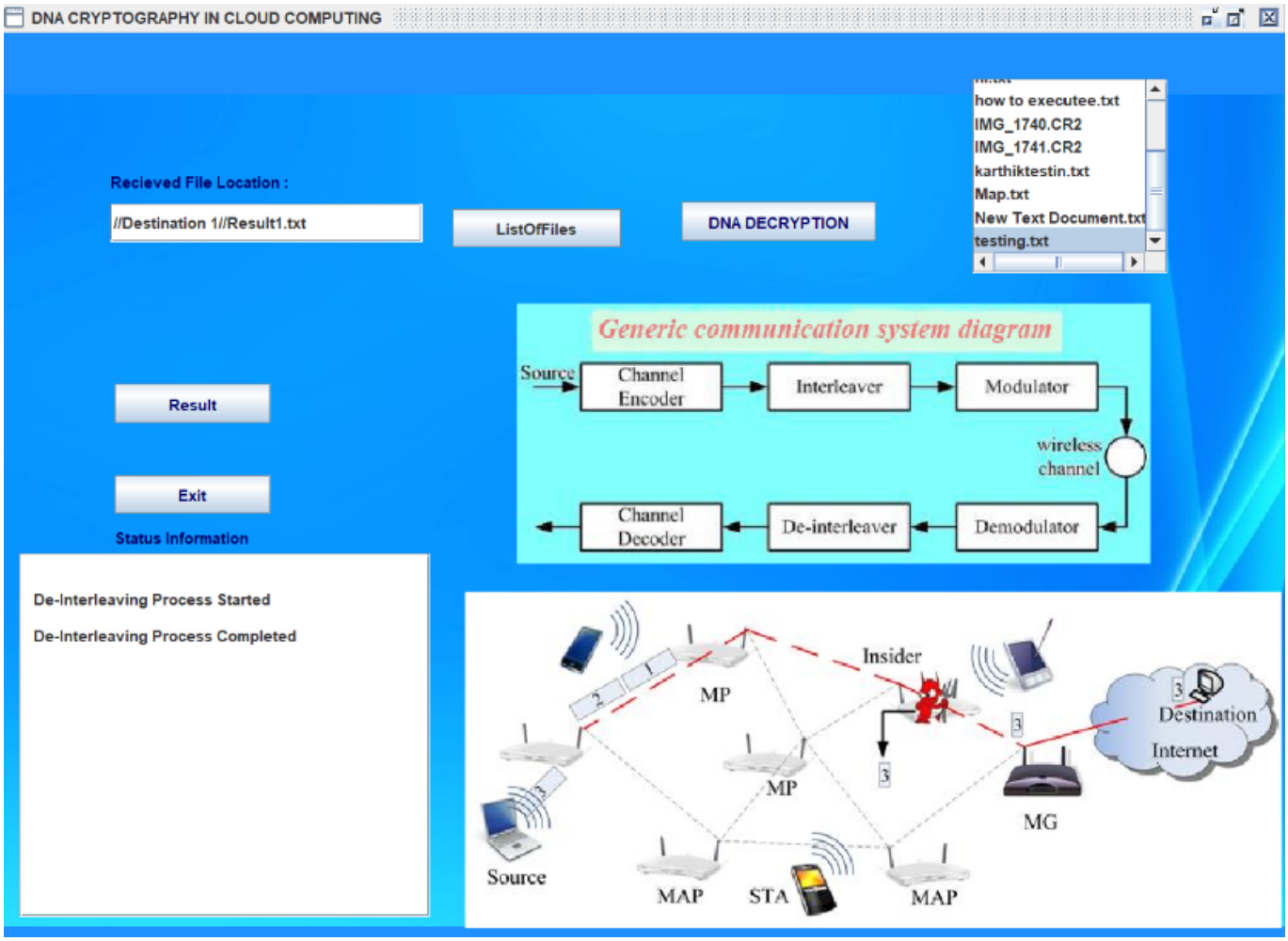

Fig 6:Decryption Process- Destination

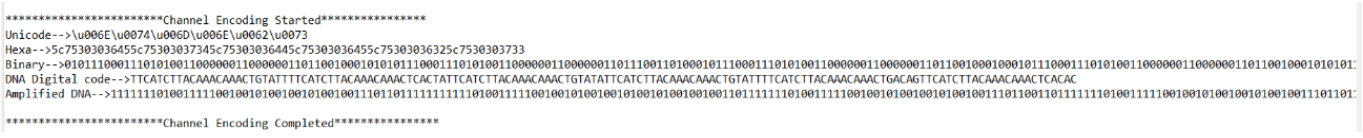

Fig 7: Encrypt / Decrypt Conversion process

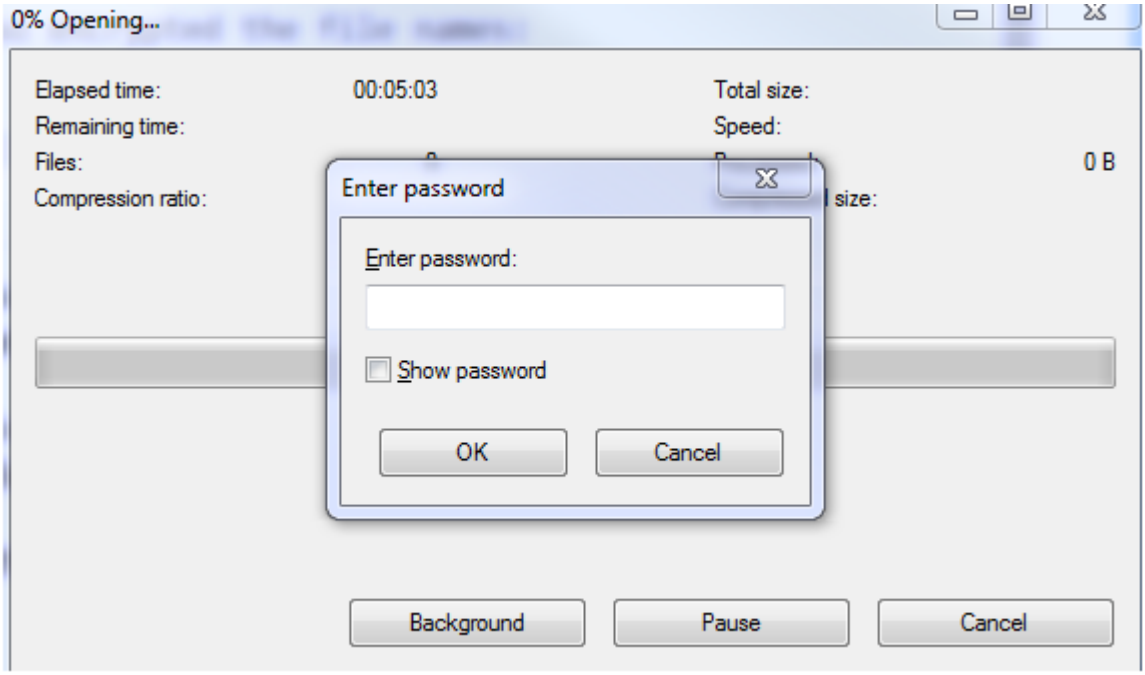

Fig 7: key needed for the folder extract

References

Mr. Harichandana Akumalla and Mr Ganapathi Hegde Deoxyribonucleic Acid Based Nonce-Misuse-Resistant Authenticated Encryption Algorithm [1]

Mr. Mehdi Hojabri and Mr. Mona Heidari Union of RSA algorithm, Digital Signature and Kerberos in Cloud Security[2]

Vinodhini R. E. and Malathi P Hiding Information in the DNA Sequence Using DNA Steganographic Algorithms with Double-Layered Security[3]

Uma Somani, Kanika Lakhani, and Manish Mundra. Implementation Digital signature with RSA Encryption algorithm to enhance the Data security of cloud in Cloud Computing [4].

Rewagad, P. and Y. Pawar. Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. In 2013 International Conference on Communication Systems and Network Technologies. 2013. IEEE.

Prajapati, A. and A. Rathod, Enhancing security in cloud computing using Bi-Directional DNA Encryption Algorithm, in Intelligent Computing, Communication and Devices. 2015, Springer. p. 349-356.

Somani, U., K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. in 2010 First International Conference On

Parallel, Distributed and Grid Computing (PDGC 2010). 2010. IEEE

Hojabri, M. and M. Heidari. Union of RSA algorithm, Digital signature And KERBEROS in cloud security. in International Conference on Software Technology and Computer Engineering. 2012.

Sowjanya, Y. and P.V.J.T. RAO, Implementation Of DNA Cryptography In Cloud Computing And Using Socket Programming. 2019. 1001: p. 9.

Rani, M. and M. Popli, A Novel Approach for Data Security Using DNA Cryptography with Artificial Bee Colony Algorithm in Cloud Computing, in Machine Learning for Edge Computing. CRC Press. p. 69-82.

Pandey, G.P.J.S.P. and N.A.t.S.C. Data, Implementation of DNA cryptography in cloud computing and using Huffman algorithm, socket programming and new approach to secure cloud data. 2019.

Namasudra, S., et al., Securing multimedia by using DNA-based encryption in the cloud computing environment. 2020. 16(3s): p. 1-19.

Kaur, M. and K. Kaur, Enhanced Security Mechanism in Cloud Based on DNA Excess 3 Codes, in Inventive Communication and Computational Technologies. 2020, Springer. p. 1-12.

Attri, J. and P. Kaur, Enhancing Cloud Security Using Secured Binary-DNA Approach with Impingement Resolution and Complex Key Generation, in Sustainable Communication Networks and Application. 2021, Springer. p. 159-171.

Reddy, M.I., A.S. Kumar, and K.S.J.B. Reddy, A secured cryptographic system based on DNA and a hybrid key generation approach. 2020. 197: p. 104207

Barman, P., B.J.I.J.o.C.I. Saha, and IoT, DNA encoded elliptic curve cryptography system for IoT security. 2019. 2(2)

Prajapati Ashishkumar B and Prajapati Barkha. IMPLEMENTATION OF DNA CRYPTOGRAPHY IN CLOUD COMPUTING AND USING SOCKET PROGRAMMING 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016

A. Mehdizadeh, M. Mohammadpoor, Z. Soltanian, “Secured Route Optimization and Micro-mobility with Enhanced Handover Scheme in Mobile IPv6 Networks”, in International Journal of Engineering (IJE), TRANSACTIONS B: Applications Vol. 29, No. 11, (November 2016) pp. 1530-1538

H. Motameni a, M. Nemati b, Mapping, “CRC Card into Stochastic Petri Net for Analyzing and Evaluating Quality Parameter of Security”, in IJE TRANSACTIONS B: Applications Vol. 27, No. 5, (May 2014) pp. 689-698

S. Karthiga, E. Murugavalli, “DNA Cryptography”, in International Research Journal of Engineering and Technology, p-ISSN 2395-0072, Vol 5, March 2018

Avani Prakasan. Avani Prakasan. Avani Prakasan, Authenticated-Encryption in the Quantum Key Distribution Classical Channel Using Post-Quantum Cryptography. 978-1-6654-1035-9, May 2022

P K Naskar and A. Chaudhuri Secured secret sharing technique based on chaotic map and DNA encoding with application on secret image, December 2016

Jenan Ayad; Fadhil Sahib Hasan; Alaa H. Ali; Zaid Khudhur Hussein; Hanan J. Abdulkareem Image Encryption using Chaotic Techniques: A Survey Study

Meera Saraswathi; K. N. Meera An Application of Radio Mean Labeling in Cryptography, December 2021

Kurunandan Jain; Prabhakar Krishnan; Vaishnavi V Rao A Comparison Based Approach on Mutual Authentication and Key Agreement Using DNA Cryptography- September 2021

Sajimon P C; Kurunandan Jain; Prabhakar KrishnanAnalysis of Post-Quantum Cryptography for Internet of Things – 2022

Shima Ramesh Maniyath1 and Supriya M An Uncompressed Image Encryption Algorithm Based on DNA Sequences -December 2021

Anupam Das, Shikhar Kumar Sarma, Shrutimala Deka. Data Security with DNA Cryptography 2019