

# **Data Encryption Technology in Network Information Security**

**BY**

**Tonmoy Sree Sagar Mondal  
ID: 221-25-107**

This Report Presented in Partial Fulfillment of the Requirements for the  
Degree of Master of Science in Computer Science and Engineering

Supervised By

**Professor Dr. Touhid Bhuiyan**  
Head  
Department of CSE  
Daffodil International University



**DAFFODIL INTERNATIONAL UNIVERSITY**

**DHAKA, BANGLADESH**

**JANUARY 2023**

## APPROVAL

This Thesis titled “**Data Encryption Technology in Network Information Security**”, submitted by **Tonmoy Sree Sagar Mondal**, ID No: **221-25-107** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 17-01-2023.

### BOARD OF EXAMINERS



**Dr. Touhid Bhuiyan, PhD**

**Professor and Head**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

**Chairman**




**Ms. Nazmun Nessa Moon**

**Associate Professor**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**

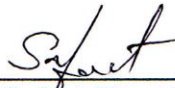


**Dr. Fizar Ahmed**

**Associate Professor**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**



**Md. Safaet Hossain**

**Associate Professor & Head**


Department of Computer Science and Engineering  
City University

**External Examiner**

## DECLARATION

I hereby declare that, this project has been done by us under the supervision of **Professor Dr. Touhid Bhuiyan, Head, Dept. of CSE**, Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

### Supervised by:

  
17/01/23  
**Professor Dr. Touhid Bhuiyan**  
Head & Professor

Department of Computer Science and Engineering  
Daffodil International University

### Co-Supervised by:



**Mr. Abdus Sattar**  
Assistant Professor & Coordinator M.Sc  
Department of Computer Science and Engineering  
Daffodil International University

### Submitted by:



Tonmoy Sree Sagar Mondal  
Id- 221-15-107  
Department of CSE  
Daffodil International University

## ACKNOWLEDGEMENT

And first foremost, we offer our heartfelt appreciation and gratitude to Almighty God for His divine gift, which has enabled us to successfully finish the final year proposal.

I really grateful and wish our profound our indebtedness to Supervisor **Professor Dr. Touhid Bhuiyan, Head, Dept. of CSE**, Department of CSE Daffodil International University, Dhaka. Our supervisor has extensive knowledge and a great interest in the subject of NLP. Deep Learning will be used to complete this project. His unending patience, scholarly guidance, constant encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages, and reading many inferior drafts and correcting them at all stages enabled us to complete this project.

I would like to express heartiest gratitude to Professor Dr. Touhid Bhuiyan, Head, Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank everyone of Daffodil International University classmates who participated in this discussion while completing their course work.

## **ABSTRACT**

Data encryption is the process of converting data from a readable format to a jumbled piece of information. This is carried out in order to prevent snoopers from viewing private data in transit. It is possible to encrypt every kind of network communication, including documents, files, communications, and messages themselves. It is impossible to overstate the value of encryption as a tool for protecting the integrity of our data. On the internet, almost all of the websites and programs we use employ some kind of encryption. This work fully exploits the public key cryptosystem's ease of key management and the symmetric key cryptographic algorithm's quick speed. The most cutting-edge data encryption methods, particularly the RSA algorithms, are suggested in this work. The data encryption system technology program is designed, and the application program is in the Windows operating system. The system provides a feasible mode of operation for the quick and secure transfer of sensitive data by fully integrating the symmetric key encryption technique and the public key encryption algorithm. It also lay the groundwork for creating a solid and comprehensive computer network security system.

## TABLE OF CONTENTS

<b>CONTENTS</b>	<b>PAGE</b>
Approval Page	i
Declaration	ii
Acknowledgements	iii
Abstract	iv
List of Figures	viii
List of Tables	ix
<b>CHAPTER</b>	
<b>CHAPTER 1: INTRODUCTION</b>	<b>1-3</b>
1.1 Introduction	1
1.2 Motivation	2
1.3 Rational of Study	2
1.4 Expected Outcome	2
1.5 Report Layout	3
<b>CHAPTER 2: BACKGROUND STUDY</b>	<b>4-6</b>
2.1 Introduction	4
2.2 Related Works	4-5
2.3 Research Summary	6
2.4 Scope of the Problem	6
2.5 Challenges	6

<b>CHAPTER 3: RESEARCH METHODOLOGY</b>	<b>7-12</b>
3.1 Research Subject and Instrumentation	7
3.2 Research Method	8
3.3 Solving Single point of Failure	9
3.4 What is the RSA Algorithm	9
3.5 Working Principle of the RSA Algorithm	10
3.6 Steps of the RSA Algorithm	11-12
<b>CHAPTER 4: EXPERIMENTAL RESULTS AND DISCUSSION</b>	<b>13-15</b>
4.1 Experimental Setup	13
4.2 Experimental Results and Analysis	13-14
4.3 Result Discussion	15
<b>CHAPTER 5: IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY</b>	<b>16-17</b>
5.1 Impact on Society	16
5.2 Impact on Environment	16
5.3 Ethical Aspects	16
5.4 Sustainability Plan	17

<b>CHAPTER 6:SUMMARY, CONCLUSION, RECOMMENDATION AND IMPLICATION FOR FUTURE RESEARCH</b>	<b>18-19</b>
6.1 Summary of the Study	18
6.2 Conclusion	18
6.3 Recommendations	19
6.4 Implication for Further Study	19
<b>APPENDIX</b>	<b>19</b>
<b>REFERENCES</b>	<b>20</b>



## LIST OF FIGURES

<b>FIGURES</b>	<b>PAGE NO</b>
Figure 3.1: Symmetric Encryption	7
Figure 3.2: Asymmetric Encryption	8
Figure 3.3: Fully Realize no Single Point of Failure	9
Figure 3.4: RSA Algorithm	10
Figure 3.5: RSA Algorithm Working Process	11
Figure 3.6: RSA Algorithm Working Steps	12
Figure 4.2: Test Data Chart	14

## **LIST OF TABLES**

<b>TABLES</b>	<b>PAGE NO</b>
Table 4.1: Result Analysis	13
Table 4.2: Results for Letter	14

# CHAPTER ONE

## INTRODUCTION

### 1.1 Introduction

The process of changing data from a readable format to a scrambled piece of information is known as data encryption. To prevent snoopers from viewing private data in transit, this is done. Any form of network communication, including documents, files, messages, and messages themselves, can be encrypted. The importance of encryption as a tool for maintaining the integrity of our data cannot be emphasized. Almost all websites and applications that we visit on the internet use some form of encryption. By definition, encryption is "the translation of data from a readable format into an encoded structure that can only be read or processed after it has been decrypted," according to renowned antivirus and endpoint security experts at Kaspersky. The public's daily life now includes extensive use of the computer network, and the resulting network information security issues also pose a threat to the public's property security and social stability. Data information encryption technology is one of the many computer network production security techniques that are more widely used and optimized. Information security for computer networks can only be prioritized as a top priority. The development of the computer network is better and faster, and it offers citizens more practical services. Data encryption technology, in short, is a development that keeps computer networks' information security technology up to date. It has the ability to convert computer-transmitted information into confidential information. The advancement of computer network information security must be prioritized. In addition to offering citizens more convenient services, the computer network improves and grows more quickly. Data encryption technology is a development that keeps computer networks' information security technology up to date, to put it briefly. It is capable of converting computer-transmitted data into confidential data. It is also possible to assure interindustry communication and enhance communication accuracy through the use of computer data encryption technology. Data encryption technology can efficiently address some computer-related issues, suggest additional and ideal solutions to maximize the

technology's functionality and scientific and technological capabilities, and offer technical support for social advancement and scientific and technological advancement.

## **1.2 Motivation**

Nowadays encryption technologies play an important role in the modern era. It assists in providing sensitive data security. Data transported via computer networks, including the Internet, and data saved on computer systems are frequently protected with encryption. Encryption is a common security measure in financial transactions and private correspondence. To ward off cyberattacks like malware and ransomware and brute-force attempts, encryption leverages cybersecurity. Data encryption secures transferred digital data on computer networks and the cloud. Digital data is divided into two categories: transmitted data and stored data.

## **1.3 Research Question**

- Will it really secure the network systems?
- How data encryption technologies will help us?
- What is Data encryption?
- Why is data encryption technologies are important?
- How do data encryption technologies work?
- How have we collected data?
- How hard was it to preprocess data?
- Did it give better accuracy?

## **1.4 Expected Outcome**

The result was that by utilizing the model, which comprises the readable text into unreadable and then again the transformed text will again convert into readable text. Here, encryption and decryption processes will be applied. With the help of this approach, the third party will not be able to read the text.

## **1.5 Report Layout**

This report varied in a total of six different chapters. Which are capable of extending the understanding of “Data Encryption” more briefly.

In the first chapter, we’ll mention introduction, motivation, rational study, research questions and the last one is the expected outcome. In the second chapter, we’ll brief about some related works, which types of challenges that we had faced and about the research summary. In the third chapter, we’ll talk about our research subject and instrumentation, workflow of the model, how we’ve Implemented RSA Algorithm. In the fourth chapter, we’ll talk about the accuracy that we got , the evaluation of our model and the comparison with other models. In the fifth chapter , We’ll describe its impact on our society, impact on our environment and sustainability. In the sixth chapter, which is our last chapter, we’ll mention the conclusion and our future works.

# CHAPTER TWO

## BACKGROUND STUDY

### 2.1 Introduction

Since internet-based crime is one of the most urgently developing security risks, encryption is more crucial than ever[1]. The most secure type of encryption, end-to-end encryption, makes sure that the private information shared online every day by billions of people stays private and out of the hands of thieves[1]. End-to-end encryption helps stop spies, terrorists, and adversarial governments from intercepting and using the private communications of public officials, as well as from hacking into computer networks and databases that could lead to widespread, systemic disruptions of economies, infrastructure, and security[1].

Additionally, law enforcement, military personnel, government officials in charge of overseeing sensitive operations, and first responders' private and confidential conversations are safeguarded by end-to-end encryption. Additionally, encryption safeguards extremely sensitive systems that are inextricably linked to national security, such as databases holding sensitive information and systems that run the electrical grid[1].

### 2.2 Related Work

The cryptographic design notion put forth by Ramamoorthy, Jayagowri, and others sparked a revolution in the field of cryptography, ushering in a new era of public key cryptography and reorienting the field. [2]. Long resistant to cryptanalysis, DES was finally broken in 1997 thanks to advancements in attack technology. Later, triple DES and deformed DES that can withstand attacks using differential analysis was developed. Triple DES is more effective than triple standard encryption and has a strength that is comparable to 112-bit keys because it encrypts data blocks three times using three separate keys. DES was formally discontinued as a standard on October 2, 2000, when NIST announced the new Advanced Encryption Standard AES [3]. The risk of network information and data theft has arisen as a result of the network's ongoing development of

its openness, which has also significantly increased people's access to information and data. As a result, individuals are becoming more and more concerned about the privacy and security of the network environment [3]. Due to this desire, data encryption is now more commonly known. Given this context, data information also needs to have high levels of secrecy and security, which can both successfully deter criminals from stealing and tampering with data information and improve users' security perceptions during data information transmission.

Data encryption is becoming increasingly vital in our daily lives, especially in light of the numerous transactions and data transfers that take place on the Internet every day. Data encryption is currently the most effective method for protecting information security. Data encryption is therefore absolutely vital and essential in ensuring data security since it allows for the hiding of sensitive information and protects the transmission security of data information. But the two sides are always the same, thus it is the same whether it is an old thing or a new one. For instance, the issue of Internet information security has caused a lot of people problems. Personal information, private information, or business data has been regularly revealed to have leaked in recent years, and the rate of leakage is rising.

Data encryption is becoming more and more crucial in our daily lives, especially in light of the daily volume of transactions and data transmission that take place online. The best method for securing information at the moment is data encryption. By using encryption technology, it is possible to preserve the security of data transfer while hiding sensitive information. Data encryption is therefore absolutely essential and critical for protecting data security.

This paper suggests a data encryption method based on network information security sharing based on current research. When using data encryption technology, a password must be set. The general population has also adopted and employed this encryption technique. This technology guarantees user security while using the network, reduces network instability and insecurity during communication, lowers the likelihood of consumer security while using the network, and ensures that purchased network services can be used independently and that user privileges can be shared.

### **2.3 Research Summary**

This paper suggests a data encryption method based on network information security sharing based on current research. When using data encryption technology, a password must be set. The general population has also adopted and employed this encryption technique. This technology guarantees user security while using the network, reduces network instability and insecurity during communication, lowers the likelihood of consumer security while using the network, and ensures that purchased network services can be used independently and that user privileges can be shared.

### **2.4 Scope of the Problem:**

I've reviewed some papers & articles. There they mentioned & applied different approaches. But my paper will suggest a data encryption method based on network information security sharing based on current research. When using data encryption technology, we have to remember always that, a password must be set. The general population has also adopted and employed this encryption technique. This technology guarantees user security while using the network, reduces network instability and insecurity during communication, lowers the likelihood of consumer security while using the network, and ensures that purchased network services can be used independently and that user privileges can be shared. So I want to implement the RSA algorithm.

### **2.5 Challenges:**

As we know, the encryption problem has become a serious issue. I thought I'll work with the help of the RSA algorithm. But it was totally new for me. So practice the RSA Algorithm, then implement it. Since encryption is simple and decryption is difficult without the private key, RSA was the first method to provide secure communication without a shared key. As a result, it is frequently utilized in secure communication on eCommerce websites.



# CHAPTER THREE

## RESEARCH METHODOLOGY

### 3.1 Research Subject and Instrumentation

In this part, I will quickly describe the steps I took to accomplish our study project. But first of all, we have to know about data encryption.

Information is changed over into another structure, or code, by means of information encryption so just those with a mystery key or secret word might interpret it [5]. Decoded information is alluded to as plaintext, while scrambled information is every now and again alluded to as ciphertext. Right now, enterprises utilize encryption as quite possibly of the most widely recognized and fruitful datum security strategies [5]. Uneven encryption usually alluded to as open key encryption, and symmetric encryption is the two fundamental strategies for information encryption [5].

Today, brute force attacks, which include attempting a variety of keys until the correct one is found, are the most fundamental way to break encryption. Obviously, the length of the key impacts the quantity of keys that may be utilized and the probability of this sort of attack [6]. It's memorable's significant that encryption strength emphatically connects with key size, however that as the key size rises, so do the computational assets required [6]. Side-channel attacks and cryptanalysis are different ways to deal with figure breaking. Side-channel assaults focus on the code's execution instead of the actual code [6]. On the off chance that there is a mix-up in the framework's plan or execution, these assaults habitually succeed [6].

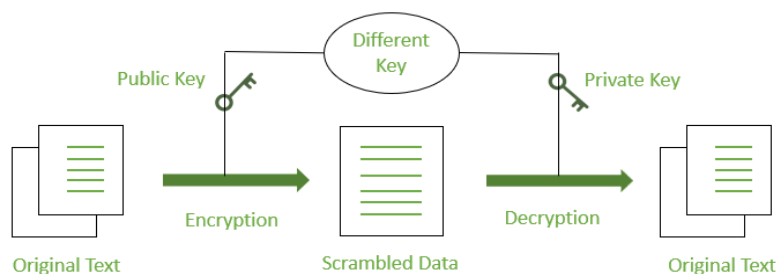


Figure 3.1: Symmetric Key Encryption [7]

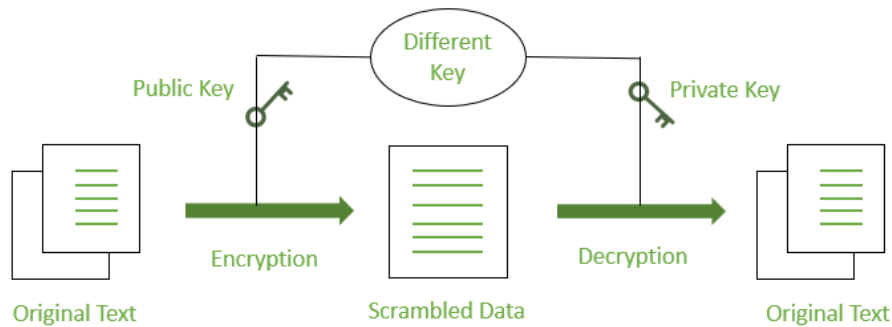


Figure 3.2: Asymmetric Key Encryption [7]

### 3.2 Procedure/Dataset Utilized

1. **Network Transmission Encryption [8]:** Their group proposes another PLC power transporter significant distance encoded transmission specialized technique in view of OTN innovation to effectively resolve the issues with PLC power transporter signal, including high decrease, short transmission distance, and simple obstruction. The establishment of an IOT exceptional exit in the space considers the organization transmission to be covered by wires at all power terminals, the bound together checking and the executives of a wide range of gadgets on the IOT cloud stage, and the evacuation of specialized obstructions like remote transmission impeding, troublesome feeble current wiring, contrariness of gear from different makers, and costly free Web access. This method makes serious areas of strength for a for the acknowledgment of PLC power transporter innovation.
2. **Data Storage Security [9]:** Due to their widespread use, constant connectivity, and variety of applications, cell phones have surpassed desktop and laptop PCs as the major computing platform. Numerous types of sensitive information can be stored on mobile devices, including images, movies, personal information, work data, and a variety of other files. As a result, protecting data saved on mobile devices turns to become a crucial issue. We examine the security of the Android

storage model between 2013 and 2018 in this review. There are a number of dangers in the literature that fall under the categories of software or physical threats. Additionally, each category's current solutions are emphasized. To improve the security of data storage, Android offers useful encryption technologies including whole disk encryption and keychain.

3. **Login Security:** The specific user can not log in 3 times a day if the password is incorrect. If she tries again and again then the account will be locked.
4. **System Logged:** Every action a user takes within the system is recorded. It primarily keeps track of user names, login times, operation modules, data updates, and system exit information.

### 3.3 Solving Single point of failure

A single point of failure (SPOF) might result in a scenario where one error or malfunction renders the entire system incapable of functioning, which creates a potential risk[10]. In the context of cloud computing, SPOFs are feasible in both software and hardware configurations[10]

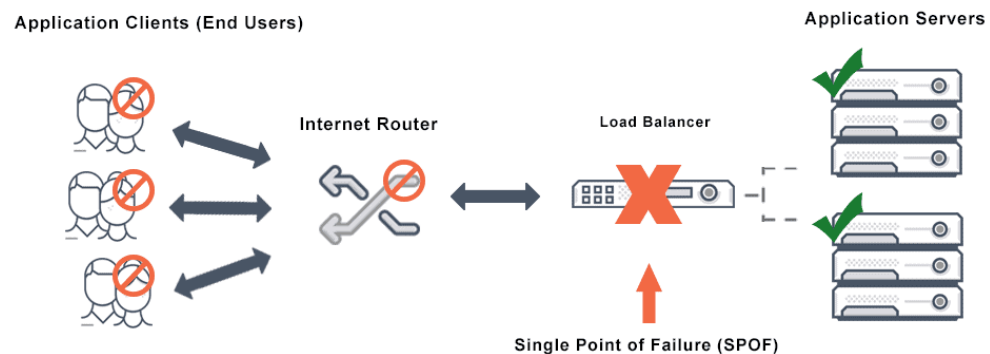


Figure 3.3: Fully Realize no single point of failure[10]

### 3.4 What is the RSA Algorithm?

The RSA calculation (Rivest-Shamir-Adleman) is the groundwork of a cryptosystem, which is an assortment of cryptographic calculations utilized for specific security administrations or purposes [11]. Public key encryption is made conceivable by the cryptosystem, which is often used to get delicate information, particularly when it is sent

over a shaky organization like the web. Albeit the 1973 improvement of a public key calculation by English mathematician Clifford Cocks was kept mystery by the U.K's. GCHQ until 1997, RSA was first openly made sense of in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Establishment of Innovation [11]. Two particular however numerically related keys — one public and one private — are utilized out in the open key cryptography, regularly alluded to as awry cryptography. Everybody can get to the public key, yet the confidential key must be the ideal individual [11].

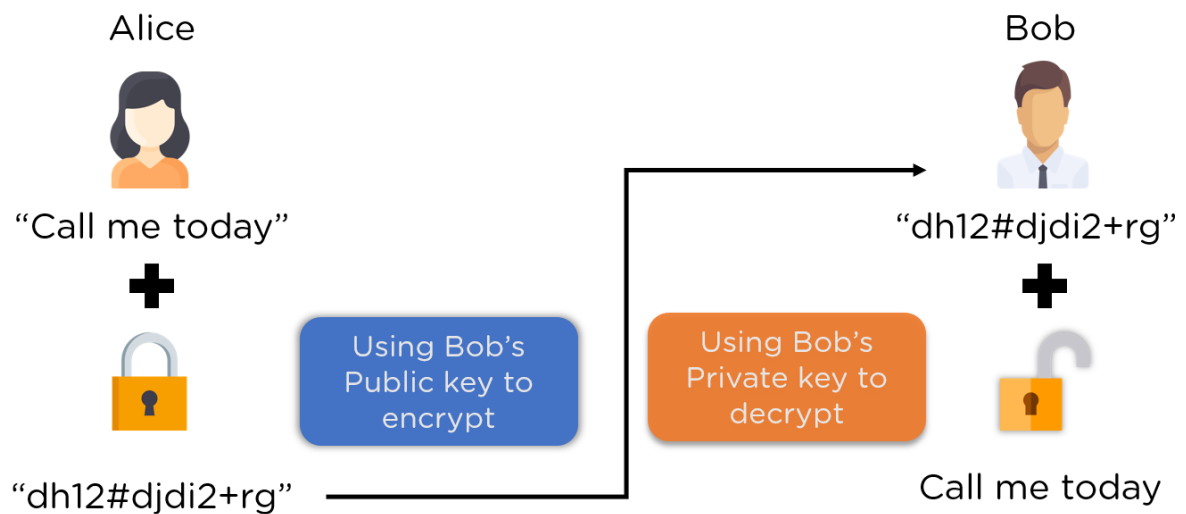


Figure 3.4: RSA Algorithm [11]

### 3.5 Working Principle of The RSA

Lopsided cryptography utilizes the RSA calculation. Lopsided truly suggests that it uses both the general population and confidential keys, which are two separate keys. As inferred by the name, the confidential key is kept mystery while the public key is dispersed to everybody. The public key is open to everyone and available as the name says. It is used to encrypt data before sending the encrypted information to a publisher of public keys [13]. The secret key is kept secret. It will not be made public and is just the publisher's property. It is the main technique for data decryption [14]. The private key

cannot be determined only through key acquisition. Data encrypted with the public key are secure and can only reach the receiver since the private key is secret. However, the RSA key length should not be too short in order to increase security and strengthen encryption; otherwise, its dependability would be impacted. The usual settings are 512 or 1024 bits [14].

## How RSA Encryption Works

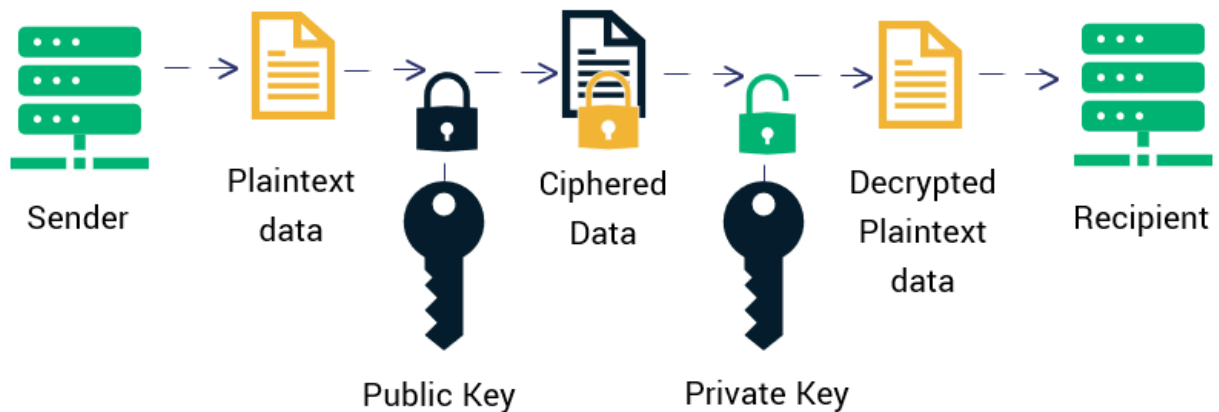


Figure 3.5: RSA Algorithm Working Process [15]

### 3.6 Steps of the RSA Algorithm

1. The initial step is to pick two indivisible numbers,  $p$ , and  $q$ , and afterward to ascertain their item  $N$ , as shown.[16]
  - a.  $N=p*q$
2. Think of the determined number  $e$  as being mutiple and not as much as  $(p-1)$  and  $(q-1)$ . The fundamental necessity will be that there ought to just be one normal component between  $(p-1)$  and  $(q-1)$  [16]
3. The public RSA key is created using the specified pair of numbers,  $n$ , and  $e$ .[16]
4. The letters  $p$ ,  $q$ , and  $e$  add up to form the private key  $d$ . [16]

$$ed = 1 \bmod (p-1)(q-1)$$

We can understand it very well with the help of a diagram.[16]

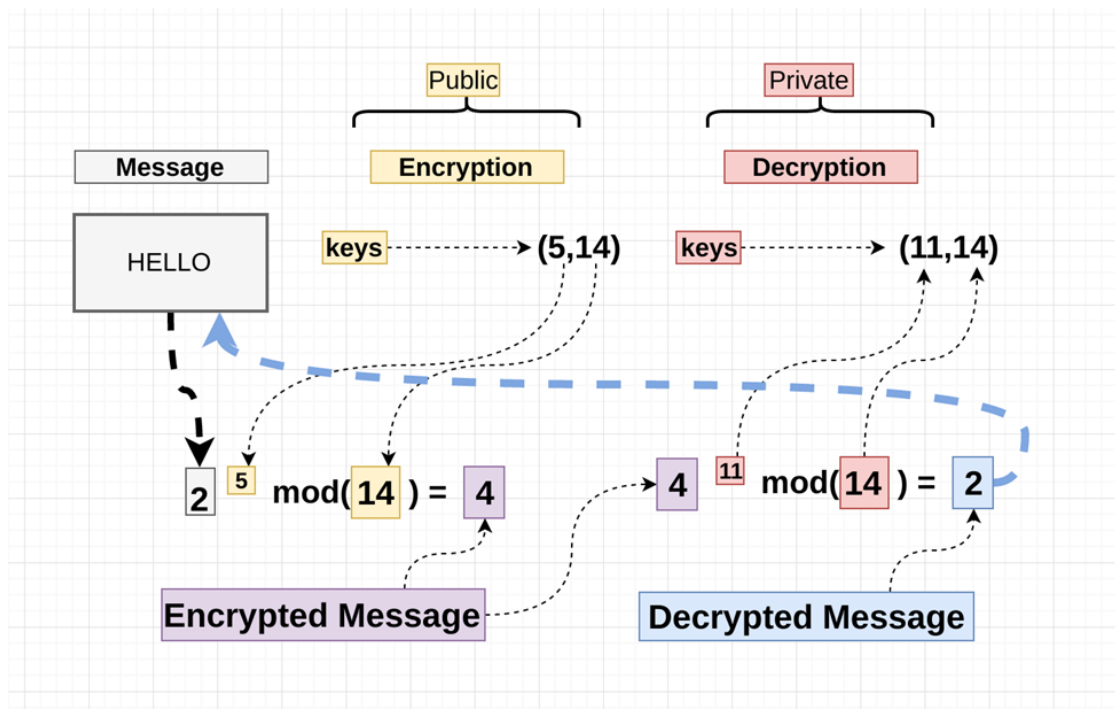


Figure 3.6: RSA Algorithm working steps

### Encryption Formula: [16]

Ponder a source who discusses in plain text with a beneficiary whose public key is [16]

$$C = P^e \text{ mod } n$$

### Decryption Formula:[16]

The unscrambling methodology is somewhat straightforward and adopts a precise strategy with examination for working out. Considering that recipient C has the confidential key d, the subsequent modulus not set in stone as.

$$\text{Plaintext} = C^d \text{ mod } n$$

## CHAPTER FOUR

### EXPERIMENTAL RESULTS AND DISCUSSION

#### 4.1 Experimental Setup

Here, we determine the more modest qualities for  $p$  and  $q$  for accommodation of computation. The qualities for  $p$  and  $q$  are 3 and 11, individually. Obviously, 33 is the worth of  $n$ , and 20 is the worth of  $(p-1)(q-1)$ . For this reason we compose it as  $f(n)$ . The worth is likewise taken to be all around as unobtrusive as attainable; subsequently, 3 is used [20]. When the qualities recorded above are perceived, the assessment equation for  $d$  is  $d \cdot e \equiv 1 \pmod{f(n)}$ . Computing the worth of  $d$  is conceivable. The worth is unobtrusive, subsequently we can decide it by means of experimentation estimations.

#### 4.2 Result Analysis

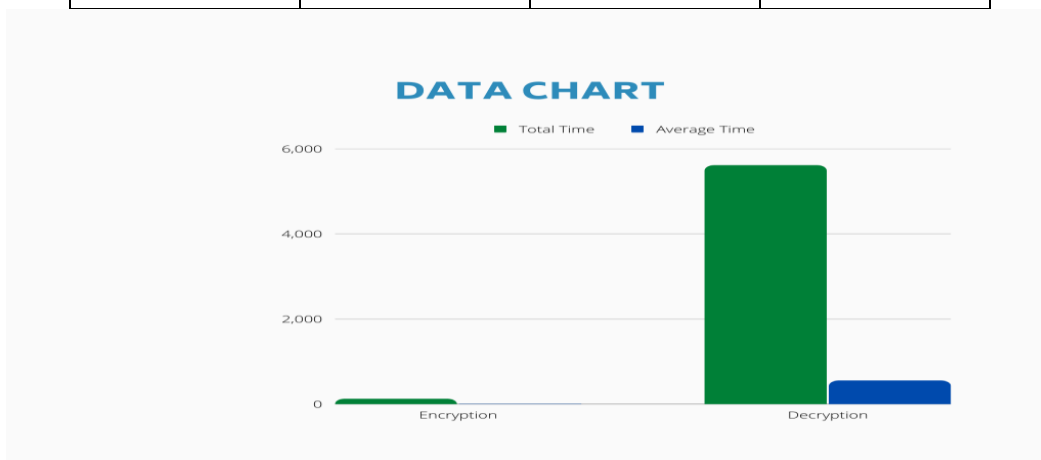
Table 4.1: Results

<b>D</b>	<b>d*e</b>	<b>d*e ≡ 1 mod f(n)</b>
1	3	3
2	6	6
3	9	9
4	12	12
5	15	12
6	18	18
7	21	1

In the trial calculation shown in the above table, we discover that the identity is valid when  $d$  is 7. Take 7 as the value of  $d$  to obtain the private key. The private key's two values are 7 and 33. The equivalent public key's two values are 3 and 33. We have created two key pairs so far. Let's check it out.

**Table 4.2: Results for letter**

Letter	Code Value	Letter	Code Value
A	1	z	1
B	2	y	2
C	3	x	3
D	4	w	4
E	5	v	5
F	6	u	6
G	7	t	7
H	8	s	8
I	9	r	9
J	10	q	10
K	11	p	11
L	12	o	12
M	13	n	13
N	14	m	14
O	15	l	15
P	16	k	16
Q	17	j	17
R	18	i	18
S	19	h	19
T	20	g	20
U	21	f	21
V	22	e	22
W	23	d	23
X	24	c	24
Y	25	b	25
Z	26	a	26



**Figure 4.2: Test Data Chart**



### 4.3 Result Analysis

The time required to encrypt and decrypt a 2.1M TXT document using a 1024-bit key pair is reported after ten rough testings [17]. The graph of the ten-test data is shown in Figure 3. As can be observed from the test above, it takes roughly 2.35 seconds to generate a key pair of 1024 bits. A 2.1 m text document can be encrypted in around 12.29 seconds using a 1024-bit public key, and it can be decrypted in roughly 561 seconds. It is suggested to use a data encryption technology based on network information security sharing. The RSA encryption algorithm is the foundation of network transmission security, cryptography, and encryption; in addition to meeting the needs of file encryption, it is thoroughly researched, examined, and put into use with software. The file encryption and decryption software has also been developed to conduct a number of in-depth experiments on the client's production key and the speed of encryption and decryption, which demonstrate that the client can completely satisfy user usage and design requirements. According to the table above, the digital codes for English keys are 11, 05, and 25. Through the use of the encryption key, the user converts the data collected in the second phase into ciphertext that is inaccessible to others (3, 33). The transformed ciphertext is obtained from. When we receive the ciphertext, we perform transformation processing in accordance with the formula, which entails decryption. As a result, we can obtain the plaintext's digital coding information as follows: To obtain the plaintext KEY, find the letters that correspond to those in Table 2.

This paper suggests a data encryption method based on network information security sharing based on current research. When using data encryption technology, a password must be set. The general population has also adopted and employed this encryption technique. This technology guarantees user security while using the network, reduces network instability and insecurity during communication, lowers the likelihood of consumer security while using the network, and ensures that purchased network services can be used independently and that user privileges can be shared.

## **CHAPTER FIVE**

### **IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY**

#### **5.1 Impact on Society**

Every human feeling may be linked to the words we view on a daily basis on various online platforms in the digital world. In this case, it is critical for these platforms to have a mechanism in place to discern which are genuine emotions and which are pre-programmed aggressiveness. This is why I've decided to focus on one of the most fascinating genres of all time,. By doing so, we can expect to create a more definitive and diverse digital era.

#### **5.2 Impact on Environment**

Due to the complexity of the network system of openness, sharing of resources, system, linking the variety, the uneven distribution of the terminal, network agnostic, and other barriers, computer networks continue to exhibit their distinctive benefits. Computer's [2] cause. The biggest issue is security, which is one of the numerous issues brought on by the network. Unauthorized access, user impersonation, data integrity destruction, system uptime interference, viruses, malicious attacks, wiretapping, and other safety issues that arise in highly open computer network environments cause significant harm.

#### **5.3 Ethical Aspects**

The internet's media outlets have now become accessible to people of all ages. As a result, the conditions of the user limitations are no longer valid. Because there are insufficient security measures to distinguish between moral and social perspectives. One must be able to comprehend the overall context of a notion conveyed through platforms. In many circumstances, this has been shown to be harmful to people's moral ideals.

## **5.4 Sustainability**

- There are over 2.3 billion active internet-based life clients worldwide.
- At least two internet-based life cycles are present in 91 percent of large business brands..
- When they can't access their online life profiles, 65 percent of individuals feel uneasy and uncomfortable.

## **CHAPTER SIX**

### **SUMMARY, CONCLUSION, RECOMMENDATION, AND IMPLICATION FOR FUTURE RESEARCH**

#### **6.1 Summary of the Study**

We believe that this work is capable of providing a new addition to the work's notion of the ongoing developmental age of Data Encryption Technologies in the wide globe where emotional intelligence is becoming more aligned with all the turbulence between our daily life structure and habits. Encryption has long been a hotly debated issue among scholars in this field, and we hope that our contribution will encourage others. So that we might create a world in which technology aids one's mind in experiencing a disaster.

#### **6.2 Conclusion**

In addition to offering citizens more convenient services, the computer network improves and grows more quickly. Data encryption technology is a development that keeps computer networks' information security technology up to date, to put it briefly. It is capable of converting computer-transmitted data into confidential data. It is also possible to assure interindustry communication and enhance communication accuracy through the use of computer data encryption technology. Information encryption innovation can proficiently address some PC related issues, propose extra and optimal answers for boost the innovation's usefulness and logical and mechanical capacities, and deal specialized help for social progression and logical and innovative headway. Here RSA Calculation was the center. The record encryption and decoding program have been made to direct various inside and out probes the client's item key and the speed of encryption and unscrambling, showing the way that the client can totally fulfill client utilization and plan rules. To give a firm confirmation for the security of information and data in transmission, various encryption procedures are utilized to scramble and decode the information during the genuine information transmission process.

### **6.3 Recommendations**

My research will help other's researcher to understand Data Encryption Technologies.

### **6.4 Implication for Further Study**

Because of the rapid growth of information available on the internet and in online social media, businesses may now use conclusion analysis to gain insight into their consumers' feelings about their products or services. In current writing, document classification is typically based on little social media data, with only a few days' worth of data. Unless social media material is routinely retrieved, this obstacle prevents the acquisition of factually significant and meaningful consequences. A broad research of tweets to develop a factually massive client evaluation must take into account a few factors.

## REFERENCES

- [1] Li, N. (2017) “Research on applications of Data Encryption Technology in security of Computer Network Communication,” *Proceedings of the 2017 5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCCE 2017)* [Preprint]. Available at: <https://doi.org/10.2991/icmmcce-17.2017.28>.
- [2] Hossein, S.M. *et al.* (2020) “DNA sequences compression by GP<sup>2</sup> R and selective encryption using modified RSA technique,” *IEEE Access*, 8, pp. 76880–76895. Available at: <https://doi.org/10.1109/access.2020.2985733>.
- [3] Eftekhari, S.A., Nikooghadam, M. and Rafighi, M. (2021) “Security-enhanced three-party Pairwise Secret Key Agreement Protocol for FOG-based vehicular ad-hoc communications,” *Vehicular Communications*, 28, p. 100306. Available at: <https://doi.org/10.1016/j.vehcom.2020.100306>.
- [4] Eftekhari, S.A., Nikooghadam, M. and Rafighi, M. (2021) “Security-enhanced three-party Pairwise Secret Key Agreement Protocol for FOG-based vehicular ad-hoc communications,” *Vehicular Communications*, 28, p. 100306. Available at: <https://doi.org/10.1016/j.vehcom.2020.100306>.
- [5] *What is encryption?* (2022) *Internet Society*. Available at: <https://www.internetsociety.org/issues/encryption/what-is/> (Accessed: November 28, 2022).
- [6] Juliana De Groot on Monday November 7, Giandomenico, N. and Lord, N. (no date) *What is Data Encryption? Definition, best practices & more*, *Digital Guardian*. Available at: <https://digitalguardian.com/blog/what-data-encryption> (Accessed: November 28, 2022).
- [7] *What is Data Encryption?* (2022) *GeeksforGeeks*. Available at: <https://www.geeksforgeeks.org/what-is-data-encryption/> (Accessed: November 28, 2022).
- [8] Graovac, J. (2014) “A variant of N-gram based language-independent text categorization,” *Intelligent Data Analysis*, 18(4), pp. 677–695. Available at: <https://doi.org/10.3233/ida-140663>.
- [9] *What is a single point of failure? definition & faqs* (2022) *Avi Networks*. Available at: <https://avinetworks.com/glossary/single-point-of-failure/> (Accessed: November 28, 2022).
- [10] Cobb, M. (2021) *What is the RSA algorithm? definition from searchsecurity*, *SearchSecurity*. TechTarget. Available at:

<https://www.techtarget.com/searchsecurity/definition/RSA> (Accessed: November 28, 2022).

- [11] Wang, Y. (2016) “Research on computer network security and encryption technology,” *Proceedings of the 2016 6th International Conference on Machinery, Materials, Environment, Biotechnology and Computer* [Preprint]. Available at: <https://doi.org/10.2991/mmebc-16.2016.22>.
- [12] Sharma, A. and Kumar, R. (2016) “Performance comparison and detailed study of AODV, DSDV, DSR, tora and OLSR routing protocols in ad hoc networks,” *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)* [Preprint]. Available at: <https://doi.org/10.1109/pdgc.2016.7913218>.
- [14] Pradeep Raj, M.S. *et al.* (2021) “Lipid data acquisition for devices treatment of coronary diseases health stuff on the internet of medical things,” *Journal of Physics: Conference Series*, 1937(1), p. 012038. Available at: <https://doi.org/10.1088/1742-6596/1937/1/012038>.
- [15] Thakkar, J. (2020) *Ecdsa vs RSA: Everything you need to know, InfoSec Insights*. Available at: <https://sectigostore.com/blog/ecdsa-vs-rsa-everything-you-need-to-know/> (Accessed: November 28, 2022).
- [16] *Understanding RSA algorithm* (no date) *Tutorials Point*. Available at: [https://www.tutorialspoint.com/cryptography\\_with\\_python/cryptography\\_with\\_python\\_understanding\\_rsa\\_algorithm.htm](https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_understanding_rsa_algorithm.htm) (Accessed: November 28, 2022).
- [17] Xu, D. and Zheng, W. (2022) “Application of data encryption technology in network information security sharing,” *Security and Communication Networks*, 2022, pp. 1–6. Available at: <https://doi.org/10.1155/2022/2745334>.

## Test-1

### ORIGINALITY REPORT

**26%**  
SIMILARITY INDEX

**22%**  
INTERNET SOURCES

**9%**  
PUBLICATIONS

**16%**  
STUDENT PAPERS

### PRIMARY SOURCES

1	<a href="https://dspace.daffodilvarsity.edu.bd:8080">dspace.daffodilvarsity.edu.bd:8080</a> Internet Source	8%
2	Submitted to Daffodil International University Student Paper	6%
3	<a href="https://downloads.hindawi.com">downloads.hindawi.com</a> Internet Source	4%
4	<a href="https://www.hindawi.com">www.hindawi.com</a> Internet Source	2%
5	<a href="https://vdocuments.site">vdocuments.site</a> Internet Source	1%
6	Submitted to University of Maryland, University College Student Paper	1%
7	Submitted to University of Westminster Student Paper	1%
8	Submitted to University of Maryland, Global Campus Student Paper	1%
9	<a href="https://www.techtarget.com">www.techtarget.com</a>	



	Internet Source	<1 %
10	Submitted to University of West London Student Paper	<1 %
11	Submitted to Deakin University Student Paper	<1 %
12	Meilin Wang. "Application Research of Data Encryption Technology in Computer Network Information Security", Security and Communication Networks, 2022 Publication	<1 %
13	Submitted to University of Cincinnati Student Paper	<1 %
14	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1 %
15	Dongzhi Xu, Wenjuan Zheng. "Application of Data Encryption Technology in Network Information Security Sharing", Security and Communication Networks, 2022 Publication	<1 %
16	Submitted to University of Florida Student Paper	<1 %
17	Mohammad Masdari, Safiyyeh Ahmadzadeh. "A survey and taxonomy of the authentication schemes in Telecare Medicine Information	<1 %

# Systems", Journal of Network and Computer Applications, 2017

Publication

---

---

Exclude quotes      Off  
Exclude bibliography    On

Exclude matches      Off