

**AN AES ALGORITHM-BASED SECURED SHORT-MESSAGE TRANSACTION**

**BY**

**TRIDIP BHOWMIK**

**ID: 183-15-11898**

**AND**

**AYSHA AKMAL**

**ID: 183-15-11959**

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

Supervised By

**Dr. Md. Ismail Jabiullah**

Professor

Department of CSE

Daffodil International University

Co-Supervised By

**Md. Tarek Habib**

Assistant Professor

Department of CSE

Daffodil International University



**DAFFODIL INTERNATIONAL UNIVERSITY**

**DHAKA, BANGLADESH**

**12 SEPTEMBER 2022**

## APPROVAL

This Project titled An AES Algorithm-based Secured Short-Message Transaction, was submitted by Tridip Bhowmik, ID: 183-15-11898, and Aysha Akmal, ID: 183-15-11959 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 B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 12th September 2022.

### BOARD OF EXAMINERS



**Dr. Touhid Bhuiyan**  
**Professor and Head**  
Department of CSE  
Faculty of Science & Information Technology  
Daffodil International University

**Chairman**



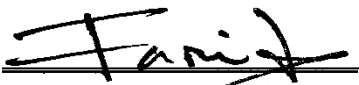
**Dr. Md. Monzur Morshed [DMM]**  
**Professor**  
Department of CSE  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**



**Ms. Samia Nawshin [SN]**  
**Assistant Professor**  
Department of CSE  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**



**Dr. Dewan Md Farid**  
**Professor**  
Department of Computer Science and Engineering  
United International University

**External Examiner**

## DECLARATION

We hereby declare that this project has been done by us under the supervision of **Dr. Md. Ismail Jabiullah, Professor, Department of CSE** Daffodil International University. We 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:**



---

**Dr. Md. Ismail Jabiullah**

Professor

Department of CSE

Daffodil International University

**Co-Supervised by:**



---

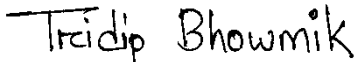
**Md. Tarek Habib**

Assistant Professor

Department of CSE

Daffodil International University

**Submitted by:**



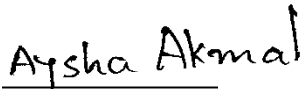
---

**Tridip Bhowmik**

ID: 183-15-11898

Department of CSE

Daffodil International University



---

**Aysha Akmal**

ID: 183-15-11959

Department of CSE

Daffodil International University

## ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to Almighty God for his divine blessing in making us possible to complete the final year project/internship successfully.

We are grateful and wish our profound indebtedness to **Dr. Md. Ismail Jabiullah, Professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “*Cryptography*” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, and reading many inferior drafts and correcting them have made it possible to complete this project.

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

We would like to thank our entire course mate at Daffodil International University, who took part in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

## **ABSTRACT**

Nowadays, the security issue is a big threat for large companies and personnel. In the digital era, people widely depended on data transactions and sharing valuable information with others. However, there are some difficulties with data transfer which are security issues. Many malicious attackers or hackers awaited users' important data to steal or destroy the data. That's why information security is the key term in data transactions. In the security world, there are even several ways and techniques used to secure communication, apathy is the better option among them. Cryptography is the technique to secure communication and prevent access to transactions from unauthorized users and intruders. The main strength of cryptography is it changes the u that it changes the user's original text format to an unreadable format that outsiders cannot understand y, there are two types of encryption processes: symmetric and asymmetric. In symmetric key-based cryptography, the same secret key is used for the encryption and decryption process. The secret key enhances the security of data transactions and is unable to crack. Only the sender and receiver know about secret keys because they are very confidential. In this research, we proposed a security system for secure data communication and ensuring data integrity based on key-based symmetric key cryptography. We apply mostly used and secured a symmetric key algorithm Advanced Encryption Standard (AES) due to the strong encryption system of this algorithm. For this reason, we used the AES algorithm to increase data integrity, confidentiality, and security.

# TABLE OF CONTENTS

<b>CONTENTS</b>	<b>PAGE</b>
Board of examiners	i
Declaration	ii
Acknowledgments	iii
Abstract	iv
 <b>CHAPTER</b>	
 <b>CHAPTER 1: INTRODUCTION</b>	<b>1-5</b>
1.1 Introduction	1-2
1.2 Objectives	2
1.3 Motivation	3
1.4 Expected Outcome	3-4
1.5 Research Questions	4
1.6 Report Layout	4-5
 <b>CHAPTER 2: BACKGROUND</b>	<b>6-12</b>
2.1 Preliminaries/Terminologies	6
2.2 Related Works	6-10
2.3 Comparative Analysis	10
2.4 Scope of the Problem	11
2.5 Challenges	12

<b>CHAPTER 3: RESEARCH METHODOLOGY</b>	<b>13-21</b>
3.1 Research Subject and Instrument	13
3.2 Proposed Methodology	13-15
3.2.1 Encryption Process	15-18
3.2.2 Decryption Process	18-20
3.2.3 Key Expansion	20
3.3 Implementation Requirements	21
<b>CHAPTER 4: EXPERIMENTAL RESULT AND DISCUSSION</b>	<b>22-26</b>
4.1 Experimental Setup	22
4.2 Experimental Results and Analysis	22-25
4.3 Discussion	26
<b>CHAPTER 5: IMPACT ON SOCIETY, ENVIRONMENT, AND SUSTAINABILITY</b>	<b>27-30</b>
5.1 Impact on Society	27
5.2 Impact on Environments	27-28
5.3 Ethical Aspects	28-29
5.4 Sustainability Plan	30
<b>CHAPTER 6: SUMMARY, CONCLUSION, AND IMPLICATION FOR FUTURE RESEARCH</b>	<b>31-32</b>
6.1 Summary of the Study	31
6.2 Conclusions	31

6.3 Implication for Further Study

32

**REFERENCES**

**33-34**

**APPENDIX**



## LIST OF FIGURES

<b>FIGURES</b>	<b>PAGE NO</b>
Figure 3.1: Proposed Encryption-Decryption System	14
Figure 3.2: Basic Structure of Encryption Process	15
Figure 3.3: SubBytes Transformation	16
Figure 3.4: ShiftRows Transformation	17
Figure 3.5: MixColumns Transformation	17
Figure 3.6: AddRoundKey Transformation	18
Figure 3.7: Procedure of Decryption Algorithm	19
Figure 3.8: Key-Expansion process	20
Figure 4.1: Output of Encryption Process	23
Figure 4.2: Output of Decryption Process	24

## **LIST OF TABLES**

<b>TABLES</b>	<b>PAGE NO</b>
Table 2.1: Comparative Analysis Between Two Models	11
Table 4.1: Output of the model	25

# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

The demand for security grew due to our increasing reliance on computers to analyze information and transmit it via virtually connected systems. Every day people deal with a huge amount of data and they need to ensure security and privacy. Organizations and individuals make transactions and share their important data through a message. People communicate with friends and others for several purposes and send important and sensitive data. However, it is not a secure way to data transfer via electric media. Hackers and third-party find opportunities to temper or steal data. Hence, people want to secure their data transactions with the help of Cryptography. It can ensure secure communication between the sender and receiver end.

The primary function of cryptography is to guarantee availability, confidentiality, and integrity. Information security and the protection of sensitive data from unwanted access are two key functions of cryptography. Cryptography has applications not just in the defense sector but also in business. Businesses and organizations utilize cryptography techniques to protect their data and information from outside threats. Cryptography has many uses in daily life and is also used to protect sensitive data. Symmetric key and asymmetric key algorithms are the two categories of cryptography algorithms. The capacity to protect data from various threats and the processing speed. If there is no way to divulge the original contents of an algorithm without the key, it is said to be secure. Therefore, the effectiveness of any safe encryption scheme is typically evaluated based on how challenging it is for cyberattacks like brute force to discover the encryption key. Large numbers have been placed together to form the keys, yet they are not identical. In the pair, the private key is kept a secret while the public key can be shared with everyone. Communication may be encrypted using either the public or the private key, and its decryption requires the opposite key. The challenge with symmetric encryption methods is maintaining the security of the secret keys once they have been transferred to each end

of the exchange. Although many well-known symmetric and asymmetric encryption algorithms, such as Data Encryption Standard (DES), Triple DES (3DES), and AES are available in the literature, there is a need for a user-friendly, straightforward, free, and all-purpose encryption tool to secure people's data transfer needs.

In this study, we design a model based on a symmetric key cryptographic algorithm to secure short messages using the AES algorithm. We used a 256-bit AES algorithm whose key length is too large than others, so it can ensure a secure transaction. The main aim of this work was to provide secure communication in data transactions. This proposed model can ensure advanced and high-performance security because of AES's strong encryption structure.

## **1.2 Objective**

Securing a data transaction between two users is a key term of the digital world. In daily life, people send lots of messages to their relatives and friends but sometimes this transaction is vulnerable. Every year a large number of companies and people lost their valuable data because of weak communication methods. As a result, we want to ensure their security using the cryptographic method between their transactions.

At present, this is the right time to use the technological revolution. Nowadays people can conduct technology everywhere, every step. Our main aim should be how securely we used technology and gain its benefits. At the same time, people should avoid technology's bad side and ensure data security.

- To secure data communication
- To prevent third parties from excess data
- To provide safety from malicious attacks
- To ensure secret transaction method
- To prevent serious and valuable information leak
- To protect against misuse of message information
- To hidden personal identity
- To establish trust between servers

### **1.3 Motivation**

Security concerns are not a new topic but it is continued from the past. People continuously lost their data or intruders access data without their permission. Advances in technology also raise the possibility of data hacking because people are now more involved in the internet. As a consequence, the security of information has also decreased in recent times. That's why we realized to ensure secure data transactions and increase data integrity. We were thinking of doing something exceptional but also helpful for general people. Then we found an idea that we will research that is based on Cryptography and we decided on a topic that is An AES Algorithm-based Secured Short-message Transaction for secure communication. We are willing to help the general people transfer data while keeping the proper data integrity, so we decided to do the work. It employs a single key for both encryption and decryption, it is quicker than most two-key methods. It provides data integrity and security. Additionally, it is simple to use and challenging to hack. It addresses the non-repudiation issue.

And finally, we reached the idea of introducing a new symmetric key encryption technique in this research. Our approach offers a higher level of security than well-known symmetric algorithms like AES while being the simplest and least complex. We have also shown that, although being extremely safe, it is not difficult to build; in fact, a straightforward implementation is quicker than many traditional algorithms. Furthermore, our algorithm offers other benefits such as data compression and the ability to select different levels of complexity.

### **1.4 Expected Outcome**

Algorithm performance depends on how much it secures transactions and is hard to crack. Furthermore, how fast one algorithm works can easily be implemented in any application. Then it will be effective and can ensure security. The main goal of our research is to ensure the followings:

- It will be helpful to increase the protection of sensitive information from unauthorized access and to provide information security.
- Our algorithm will be faster and simple, ensuring data security and integrity.
- The proposed method can be used in a variety of business and other settings where data security and confidentiality are important because it is simple to use and hard to crack.
- It will enhance the confidentiality of sensitive data

## **1.5 Research Question**

It was quite difficult for us to complete this assignment and come up with multiple research topics. We keep these following inquiries in our mind to succeed. We focus on the following question and try to solve this.

- Which type of information or data need to encrypt?
- How complicated key do we use?
- Which algorithm will be more secure?
- Can we increase the robustness in AES?
- How to transfer data securely and fast?

## **1.6 Report Layout**

There are six chapters in this report and every chapter discuss different aspects. In this section we summarize this:

Chapter 1 discussed the introduction, motivation, objectives, research questions, and expected outcome of the study.

Chapter 2 provides a discussion on the background of the work as well as covers related works, comparative analysis, scope, and challenges.

Chapter 3 discuss the methodology of the project and require equipment and software to implement the project.

Chapter 4 provides the overall results of the project and proof of the result and also describes the discussion of the study.

Chapter 5 discuss the impact of the project on society, the environment, ethical aspects, and the sustainability plan.

Chapter 6 presents the conclusion and summary of the project.

## **CHAPTER 2**

### **BACKGROUND**

#### **2.1 Preliminaries/Terminologies**

Secure communication is one of the trendsetting topics currently being addressed by scientists and researchers. Many security experts are now working in this field and want to develop a more secure transactional model. Moreover, many models already exist and are proven in the digital environment. Securing a data transaction between two users is an important term in the digital world. Numerous companies and people lose important data every year. Therefore, we wish to assure their security by the use of cryptography in their transactions. Cryptography is the most effective way to keep our information secure. By using Cryptography plays a significant role in computer security by using encryption and decryption methods to send and receive information main goal is to address this security issue. We will research further relevant work about these issues to results.

#### **2.2 Related Works**

Investigate and compare the reliability of the RC4 and FJ-RC4 and increase the security of RC4 by introducing a new algorithm KSA. F.J. Kherad et al., [1] proposed a new self-developed symmetric algorithm called FJ-RC4 derived from RC4. Used the RC4 algorithm to develop a cipher called FJRC4. FJRC4 built a new KSA. The encryption and decryption phases use the RC4 symmetric algorithm, which uses the key in three stages and shares PRGA structures with RC4. A similarity between FJRC4 and RC4 algorithms for the encryption and decryption using key stream and combining the plain text with the cipher text. They have proposed a new algorithm using a single key for both encryption and decryption, and it's better than a low-level algorithm besides the classical algorithms. A. Anand et al., [2] the new cryptographic encryption algorithm using plain text converts into upper case. Each character extracts one by one performs level 1 (convert blank and even spaces to \$ and #), level 2 (switch all alphabets B with Y), and finally level 3 (repeat switch the second alphabet and then append with the ASCII char). For decryption, receive cipher



text, convert it into upper case and extract each character. It provides layered security to protect data integrity, simplicity, and efficiency of information.

This system examines recognizing phrase search over highly encoded cloud information with a symmetric key primarily based check. T. P. Anithaashri et al., [3] proposed a system that investigates achieving watchword search over compelling encoded cloud data with symmetric encryption. Then processed data verify with the proper key, which is the confirmation of authentication. This authentication helps symmetric key cryptography convey data protection in the cloud. System architecture defines the structure, behaviors, and dynamic information. System authentication tag provides symmetric key cryptography to make an association in fostering a blend assertion tag for each watchword. Establish a higher level of security, one simplest software implantation using an alternate symmetric key encryption algorithm that can avoid a long and complex computation of conventional symmetric encryption key and provide high-speed performance. A. Murtaza et al., [4] The proposed encryption approach are about the theory of using the data encoding technique. The encryption process generates random numbers using permutations to encode the data, and the receiver can quickly shuffle the decoded data to get the original data accurately.

The AES encryption and decryption use the architecture with low complexity. It is used for hardware applications or smart cards. C.C. Lu et al., [5] have designed modules that can be used in S-box operation, TSMC, SubBytes, and KeyExpansion and are capable of use in encryption and decryption of AES. There hardware implementation of SubBytes and InvSubBytes has decreased by 57% compared with the original hardware requirement without the functional integration. This paper extended the AES algorithm from 256 bits to 512 bits. It increases the efficiency to protect against attack by around 230%. R. Jain et al., [6] This AES 512 overcomes the drawbacks of previous AES 256 where 256 bit is used which can be prone to different types of attacks. To shield against attack, 512 is used instead of 256 bits. This model presents two Rijndael AES encryption for the key length of 128 bits and compares the algorithm in two hardware SOPC and HDL models. O. Elkeelany et al., [7] implementation of Rijndael AES algorithm using a symmetric key

block cipher encryption and decryption. Firstly, input is copied to the state array using a secret key, then encrypts and decrypts the reverse operation based on HDL and IP core hardware model. This system sends messages to a secure channel on the Android platform. R. Rayarikar et al., [8] This application platform are friendly, fast, and strong to crypt the data. The cipher key is used to encrypt and decrypt the message for secure communication. These application features are pattern lock, thread view, display settings, tone settings, and notification. Maintain the information as per user specifications. Message transaction medium uses BTS transceiver, GSM/CDMA, MSC, and SMSC.

In this paper, a combination of Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) obtains a hybrid encryption model. M.O. Onyesolu et al., [9] The system stores new encrypted data in the database. Use one secret key for encrypting and re-encrypting the cipher text using another 3DES algorithm with the help of key number 2. Store decrypted data using a 3DES algorithm with a secret key 2. Data for authorized users only before decrypted, the output of the 3DES uses an algorithm for AES with key 1. Comparing AES and 3DES, the hybrid (FHES) algorithm takes significantly more time for both encryption and decryption. The software processor for system initialization and control, and the hardware AES engine for high-performance AES encryption/decryption. M. Biglari, E. Qasemi, et al., [10] The architecture presented in this document is highly modular and developed for the specific platform. They proposed two new technologies in the design of the AES engine that allow it to achieve a performance of 12.8 Gbps. First, the closely coupled encryption and round key generation units in the encryption unit, and second, the generation of round keys in advance in the decryption unit. An FPGA card with better memory bandwidth would improve outcomes.

Propose a symmetrical key cryptographic system based on a genetic algorithm (GA) for encrypting and decrypting. Sindhuja K et al., [11]. The objective of the algorithms is the right shift, matrix addition, module operation, and DNA operations. Design phases use Matrix Addition, Substitution, Genetic crossover, and mutation. The process of generating keys and the intermediate encryption algorithm offer good security to the transmitted data. Here, a symmetric key substitution algorithm is used to ensure confidentiality within networks, which is combined and implemented using genetic functions to provide extra

security. This application can be used as a basis for designing a built-in communication system for a military organization. N.G. BARDIS et al., [12] The basic tenet of a symmetrical cryptographic communication system is the user of a shared secret key that is used for both encryption and decryption. The user gets their keys from other users of the same group, with which they can decrypt the corresponding messages. Every communication period has a different communication key. Application implementation details include a Visual Basic six implementation developed for a military unit. Provide a fast and secure encryption algorithm utilizing substitution mapping, translation, and transposition operations. V. Shokeen et al., [13] Matrix-based substitution gives rise to polyalphabetic cipher text generation followed by conversion based on multiple round tables and, X-OR logical translations giving strength to this encryption algorithm. Decrypting encrypted messages created using this encryption is virtually impossible through extensive key searches, as with other algorithms using the 128-bit secret key. This feature also makes decoding extremely difficult due to brute force.

In the AES algorithm, the number of turns involved in cipher and decryption depends on the length of the key and the number of block columns. S. Radhika et al., [14] Increase key length to 512 bit the strength increases and to achieve it the total round also increased. The number of turns is increasing; it enhances the complexity of the algorithm making it powerful against cryptographic attacks. Thus, increasing the size of this key gives the AES algorithm strong resistance against new attacks and has an acceptable speed for data encryption and decryption. S. Radhika et al., [15] propose a new encryption algorithm based on several mathematical terms, formulas, and operations. This application is called Secure Text. However, the algorithm is a symmetrical encryption algorithm that can quickly encrypt a particular file and is sufficiently robust for a variety of purposes like .txt, .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .png. The current project uses standard methods of attribute encryption to generate data using the user's key in an encrypted format. Shravani et al., [16] The modules included in this project are Admin, User, File Upload, Secure Key, Authentication, and Download File. The owner of the file may keep this data encrypted. For the data, the owner must have a secret key. Using pyAesCrypt encryption, the concept of the secret key approach is implemented. When the administrator uploads a

file, the database saves the data, and the admin can identify who needs to access the encrypted file or not.

The suggested technique provides excellent encryption quality. R. Padate et al., [17] Using the modified AES key expansion approach described above, the sender and receiver may now produce the keys necessary for the operation separately. Encryption is done in spans, with each span processing, 16 pixels, and the decryption technique is identical to the encryption procedure, except that we employ inverse SubByte transformation. This paper is about SMS encryption for mobile communication using the android message app. Suriyani Ariffin et al., [18] This paper is about SMS encryption for mobile communication using the Android message app. The usage of the 3D-AES block cipher symmetric cryptography algorithm for SMS transfer security is proposed in this paper. According to the results of the experiment, the 3D-AES has a short encryption time when the message size exceeds 256 bits. The results show that the suggested approach is appropriate and simple to apply to mobile devices. This research investigates the performance of the Rijndael AES Encryption method with a key length of 128 bits. O. Elkeelany et al., [19] compared the algorithm's performance in two hardware-based models. SoPC-based hardware model and Verilog HDL-based Single Core HDL model. The evaluation findings reveal that the single-core HDL model is faster and more efficient than the SoPC-based approach. Finally, they discovered that utilizing the identical target hardware device, a single-core HDL model is 27 times quicker than a SoPC hardware model.

### **2.3 Comparative Analysis**

In the area of cryptography, there are numerous encryption models accessible. Many security researchers and analysts create methods to protect communication using their systems. Different key lengths and strategies were suggested by each professional for their security system. Significant encryption techniques, however, fall short of their goals because the encryption system has some flaws. This section contrasts our suggested system with one that already exists. The SMS encryption system on an android platform developed

by R. Rayarikar et al. [8] is based on the AES algorithm. They designed an encryption model using the AES algorithm on the android platform. They focused on the AES 128-bit encryption algorithm for their system but we used the AES 256-bit encryption algorithm. Here, we compare some significant features between the two models and demonstrate the weakness and strengths of the system. We take into account a few features and how they fare against these standards for this comparison. Table 2.1 represents the comparative analysis of the proposed system and existing system.

Table 2.1: Comparative analysis between two model

Feature	Existing model	Proposed model
Authentication	Yes	Yes
Integrity	Yes	Yes
Time Complexity	High	Low
Key Length	Shorter	Larger
Complexity	High	Low
Implementation	Only on the android platform	Any platform and system

## 2.4 Scope of the Problem

Our objective is to develop a more effective method for ensuring the security and integrity of data. High encryption quality is maintained by our suggested approach. As of right now, there is no proof that the AES is impervious to attacks other than the kind that may be carried out by brute force searching through extensive databases. Even the AES-128 offers enough possible keys, which makes exhaustive searching impossible for many decades. The algorithm was successfully applied and tested for text encryption.

## 2.5 challenges

The principal challenge is which algorithm is suitable for our work because they are various symmetric algorithms developed for encryption and decryption, like image encryption using scan patterns. But they have their limitations. Also, some algorithms were not

suitable for real-time applications as the algorithm had high security but was slow in processing. So finally, we chose the AES symmetric key algorithm for encryption and decryption. The AES algorithm was designed to resist all known attacks, be fast, be code compact, work on a wide range of platforms, and be easy to understand. They can deliver SMS or text files at a high data rate in encryption/decryption operations.

## **CHAPTER 3**

### **RESEARCH METHODOLOGY**

#### **3.1 Research Subject and Instrument**

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. We used cryptography to protect user data and make an adverse model for the transaction. As This Research Follow “An AES Algorithm-based Secured Short-Message Transaction” our goal is to protect data transaction in the digital world and provide a secure method to do that. In this paper, we have used Symmetric Key-Based AES Algorithm. A symmetric key algorithm uses the same key K to perform the Encryption and Decryption process. It generates cipher text from plaintext and again returns the original plaintext to the receiver. We used JavaScript to implement the AES algorithm and HTML, and CSS to implement this algorithm in the web browser. We develop a model using a web application to demonstrate our system.

#### **3.2 Proposed Methodology**

The proposed adverse communication model is based on symmetric key cryptography. The basic operation principle for a system of symmetric cryptographic communication is the use of a shared secret key that is used for both the encryption and decryption process. It is also known as private key cryptography. The secret key is the most important component of the encryption system, as it is the principle means that transforms clear messages into ciphertexts. In the present day, AES is the most popular and used algorithm for its security and faster encryption and decryption process for faster data communication. For example, one research shows that the AES algorithm is six times faster than also DES algorithm. AES (Advanced Encryption Standard) keys are symmetric keys that can be of three different key lengths AES-128, AES-192, or AES-256 bits. In this project, we will use the AES-256 standard AES Algorithm. This is because the AES 256-bit encryption algorithm uses a large key length than AES 128-bit and AES 192-bit. That characteristic makes it more complex and secure. The AES algorithm transforms valuable data and makes it

indecipherable to hackers and other individuals attempting to access your data without authorization. AES algorithm uses a special structure to encrypt data to provide the best security. That's why in this proposed system we prefer to introduce the AES algorithm. In this proposed model there are two ends: sender and receiver. The encryption process occurs in the sender and the decryption process happened in the receiver end.

In the encryption process, the sender sends 256-bit plain text to the receiver which is easy to read. This text passes into the encryption algorithm for encrypting the data and we used a 256-bit secret key for encryption. After the process, the encryption algorithm generates the ciphertext, which is made up of seemingly random characters. It is impossible to read, so hackers can't use this text or do not understand what message the sender sends. Therefore, in decryption process uses the same key that was received from the sender side. The decryption processes of an AES used the inverse mode of the encryption process and use the same key which is used for the encryption process. At first, the cipher text enters the decryption algorithm here we used the same secret key for decryption. After completing this process receiver can see the original text. Without a secret key, anyone cannot decrypt the cipher text. Figure 3.1 demonstrate the proposed encryption-decryption process.

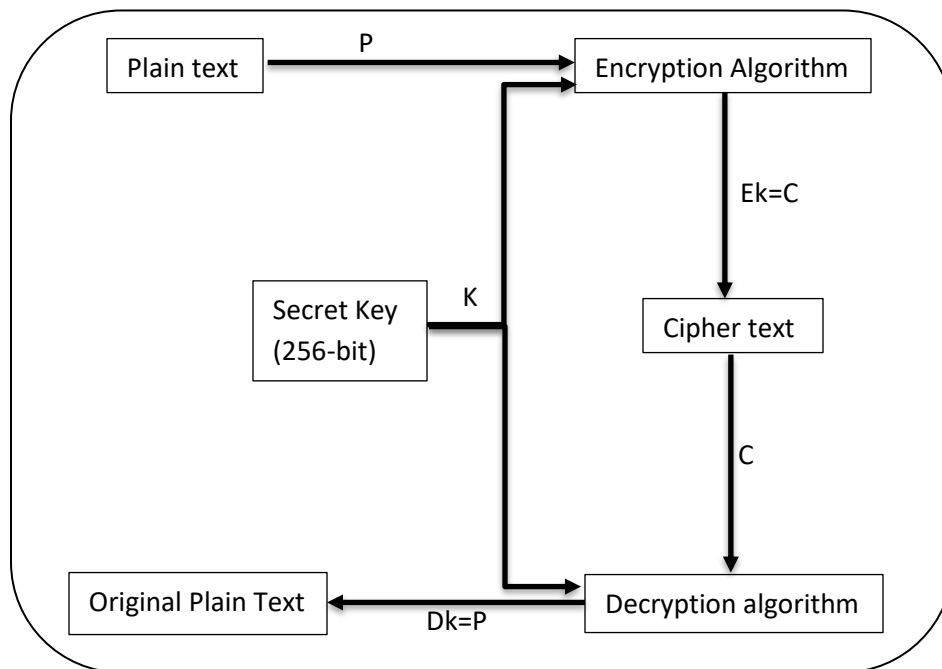


Figure 3.1: Proposed Encryption-Decryption System



### 3.2.1 Encryption Process

Encoding data is the process of encryption in cryptography. This process converts original text to unreadable text that's why unauthorized users cannot easily understand the what sender sends to the receiver. The Advanced Encryption Standard (AES) is wide used symmetric-key algorithm for encryption information. The AES cipher is defined as a series of transformation rounds that change the input plaintext into the desired ciphertext at the end of each round. AES encryption technique depends on the length of the key, while we used a 256-bit key in the proposed model. In the AES encryption technique, there are different types of transformation rounds such as AES 128-bit uses 10 rounds, AES 192-bit uses 12 rounds and AES 256-bit uses 14 rounds. That's why our proposed AES encryption algorithm will use the 14 rounds transformation technique. Every round consists of four different steps such as AddRoundKey, SubBytes, ShiftRows, and MixColumns. The MixColumns step will be missing in the last round of the algorithm. Figure 3.2 will show the basic structure of the AES encryption process.

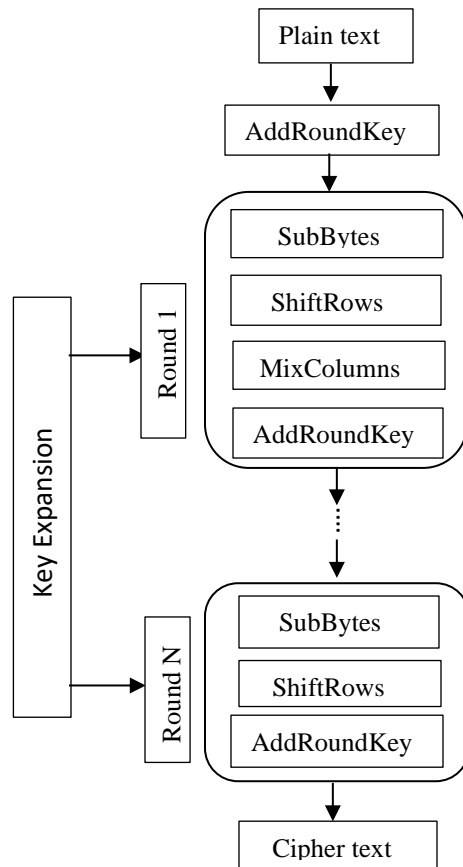


Figure 3.2: Basic Structure of Encryption Process

Now we will explain every step of the encryption process separately with a proper description. SubBytes, ShiftRows, MixColumns, and AddRoundKey follow different functionality and encrypt the data.

**Step-1:** SubBytes transformation occurs first in each round. A non-linear byte transformation in which each byte is replaced with one from another and is then brought to a conclusion by an S-box function. An S-box transformation is one in which all of the substitution transformations are finished in a single clock cycle and the total number of substitution boxes contains a 4x4 matrix. Figure 3.3 demonstrates the SubBytes transformation.

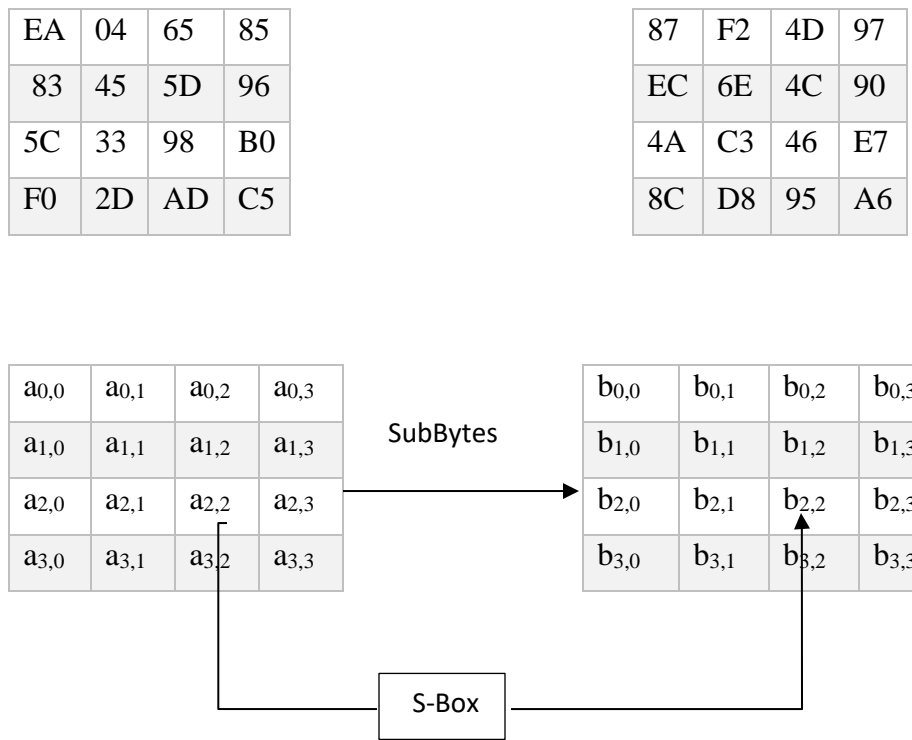


Figure 3.3: SubBytes Transformation

**Step-2:** ShiftRow is the second step of the round. The first row remains the same during this operation. One byte is rotated into a shift left in the following row. In the third row, two bytes are rotated to the left and in the fourth row rotated three rows to left. Figure 3.4 will show the process of shiftRows.

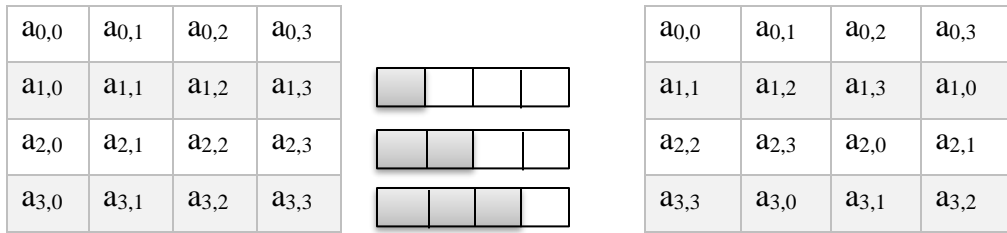


Figure 3.4: shiftRows Transformation

**Step-3:** The MixColumn transformation is the third stage of this process. Each byte in the matrix transformation is multiplied with each column value in this stage, which involves matrix multiplication. The output of the multiplication is combined using the XOR technique to create a new matrix of four bytes for the following step. Figure 3.5 will represent the AES MixColumns process.

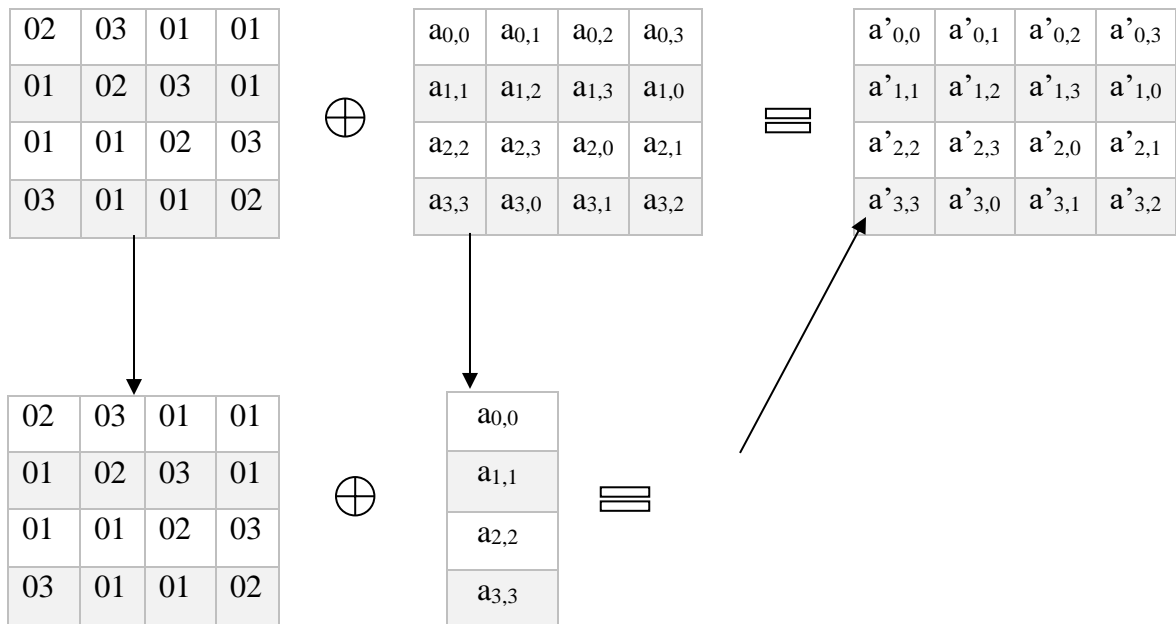


Figure 3.5: MixColumns Transformation

**Step-4:** AddRoundKey is the final step. The crucial component of the AES algorithm is AddRoundKey. Here, the AddRound key is added to the output of the Mixcolumn

transformation via a straightforward XOR operation. One distinguishing key that is derived from the main key is used for each round. As a result, 14 rounds are performed using 15 unique keys that were generated from cipher keys. The plain text is then encrypted using 14 rounds and we attained ciphertext at last. Figure 3.6 shows the AddRoundKey transformation of the AES encryption algorithm.

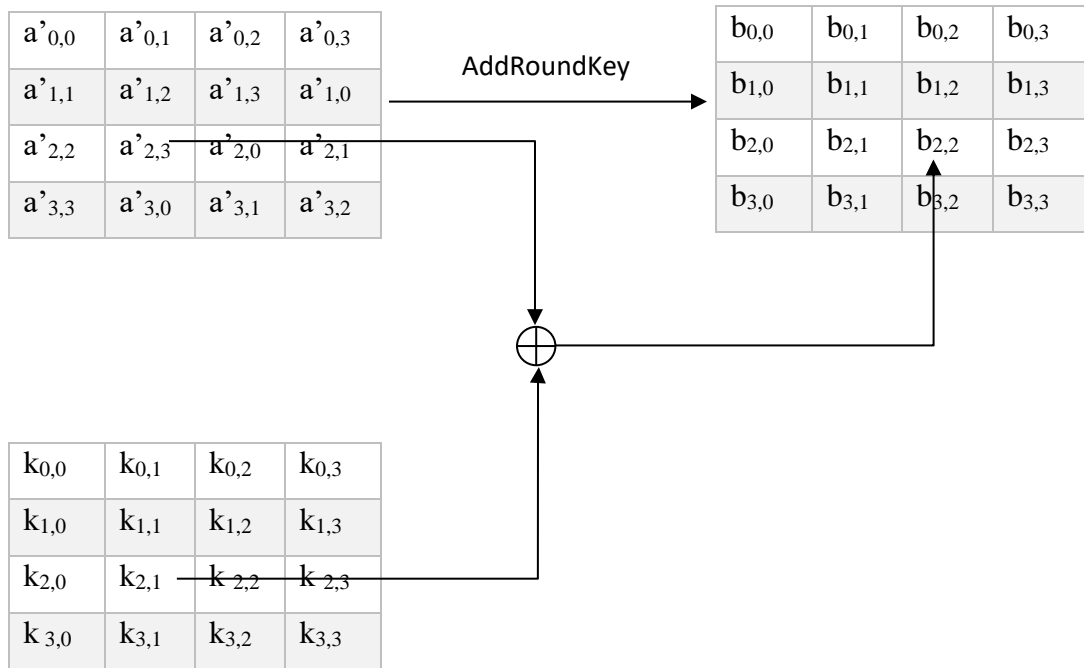


Figure 3.6: AddroundKey Transformation

### 3.2.2 Decryption Process

The decryption process decodes the cipher text and converts it to original plain text. While the encryption process is over encrypted text passes to the receiver end. The same key that was obtained from the data sender is used during the decryption operation. The decryption processes of an AES used the inverse mode of the encryption process and use the same key which is used for the encryption process. The processes involved in decryption include inverse SubBytes, inverse ShiftRows, inverse Mixcolumns, and AddRoundKey. Three stages InvShiftRows, InvSubBytes, and AddRoundKey, are performed in the final round of a decryption method. This round's version of Mixcolumns Step is invisible. Here, the decryption process will also perform 14 rounds of transformation as a link as an encryption

algorithm. The ciphertext is fed into the decryption algorithm, which decrypts the data using the same secret key. Following data decryption, the technique generates original plain text, which the sender then sends to the recipient. Figure 3.7 demonstrate the procedure of the decryption algorithm.

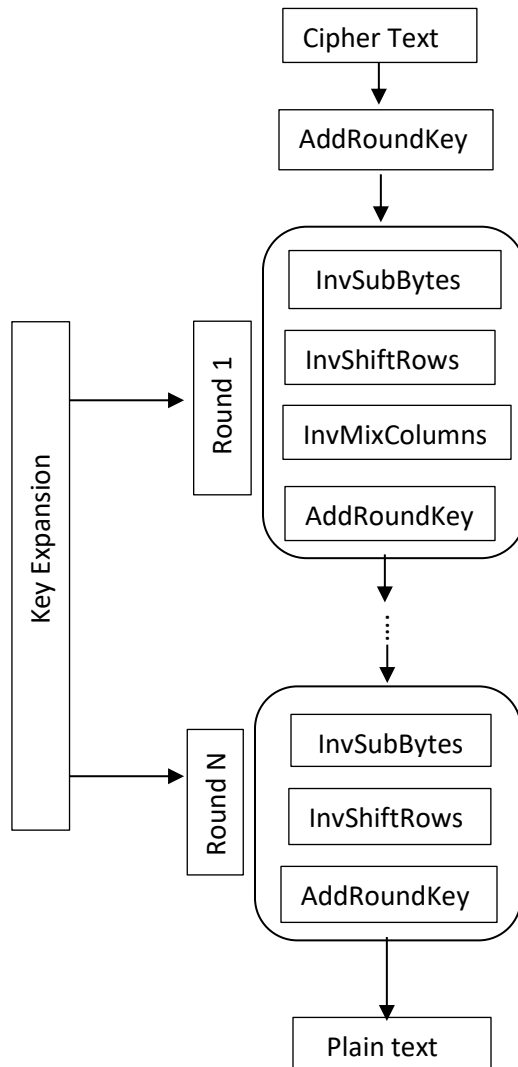


Figure 3.7: Procedure of Decryption Algorithm

### 3.2.3 Key Management

Key is the key component in cryptographic security systems because encryption and decryption systems relied on a secret key. Additionally, depending on how strong and intricate the key is, the strength of the adversaries' model will vary. One key, referred to as a shared secret, is used for both encryption and decryption in symmetric encryption, which is also known as secret key encryption. To improve information security and lower the chance of the secret key being cracked, we employed a secret key that was generated at random for both encryption and decryption in the suggested paradigm. This is due to the increased likelihood of key disclosure among invaders if we utilized a fixed key for every encryption. We suggest generating a secret key at random for each transaction to get around this problem. Permanent keys are used in the majority of current models, however, ours does not. We believe it will contribute to making our system more secure. Figure 3.8 will represent the key expansion of the AES algorithm.

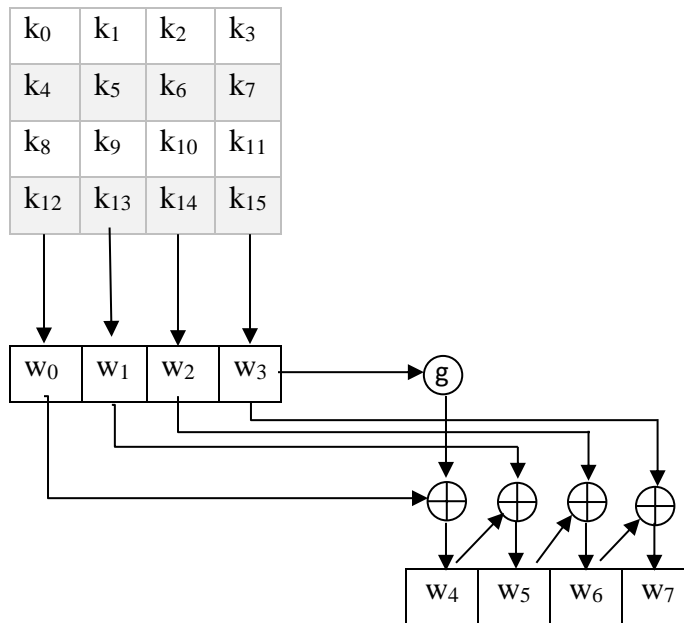


Figure 3.8: Key-Expansion Process

### **3.3 Implementation Requirements**

Implementing this model needs a highly configure PC and setup, and also needs programming language for implementing the algorithm. Required some instruments to complete this task and below list of the necessary component and equipment, we used in this work.

#### **Algorithm requirements:**

- Plaintext as text
- Secret Key
- Strong algorithm for encryption-decryption (AES)

#### **Developing Tools and Language:**

- Visual Studio
- JavaScript
- HTML
- CSS

#### **Hardware/Software Requirements:**

- Operating System- Windows
- Google Chrome
- RAM (8GB)
- Hard Disk (500GB)

## **CHAPTER 4**

### **EXPERIMENTAL RESULTS AND DISCUSSION**

#### **4.1 Experimental Setup**

To implement this experiment, we need to use a high configure and powerful setup. This is because cryptographic algorithms conduct complex calculations and their key generation is complex that's why need a highly configure PC and CPU. We used Windows 10 as an operating system. For the encryption and decryption process minimum of 4GB Ram pc or laptop is needed otherwise it can't work properly. Because there is a need to encrypt-decrypt data and pass information between two users. That's why we used an 8GB RAM laptop and 1TB hard disk. To implement the algorithm use used visual studio and we used JavaScript to implement the algorithm. Moreover, we design a webpage using HTML and CSS to visualize the overall working process and check how its input and output act. And finally, we used our algorithm behind the webpage.

#### **4.2 Experimental Results and Analysis**

We go over the overall result and performance of our suggested system in this part. The effectiveness of the encryption and decryption systems determines how well this algorithm performs and produces results. To demonstrate our proposed model, we used the AES encryption algorithm. The AES algorithm security method is the strongest and most difficult to crack of all the cryptographic algorithms. Because the AES algorithm's key is longer and more complex than other symmetric key algorithms, outsiders are unable to decipher the messages being sent. When people send a message to other ends it encrypts this text and keeps it secret. Similarly, encrypted messages when passed to the receiver end then it will decrypt and people get the original text. The efficiency of the algorithm was better than another algorithm.

For encryption purposes, here we use the text "AES Encryption-Decryption Process" as plain text and send our text to the receiver end. For this reason, plain text is placed onto the



encryption algorithm, which is used to encrypt the plain text using the secret key “Symmetric Key”. Then we get a cipher text in other formats of text which is unreadable and difficult to understand. Figure 4.1 demonstrate the result of the encryption process.

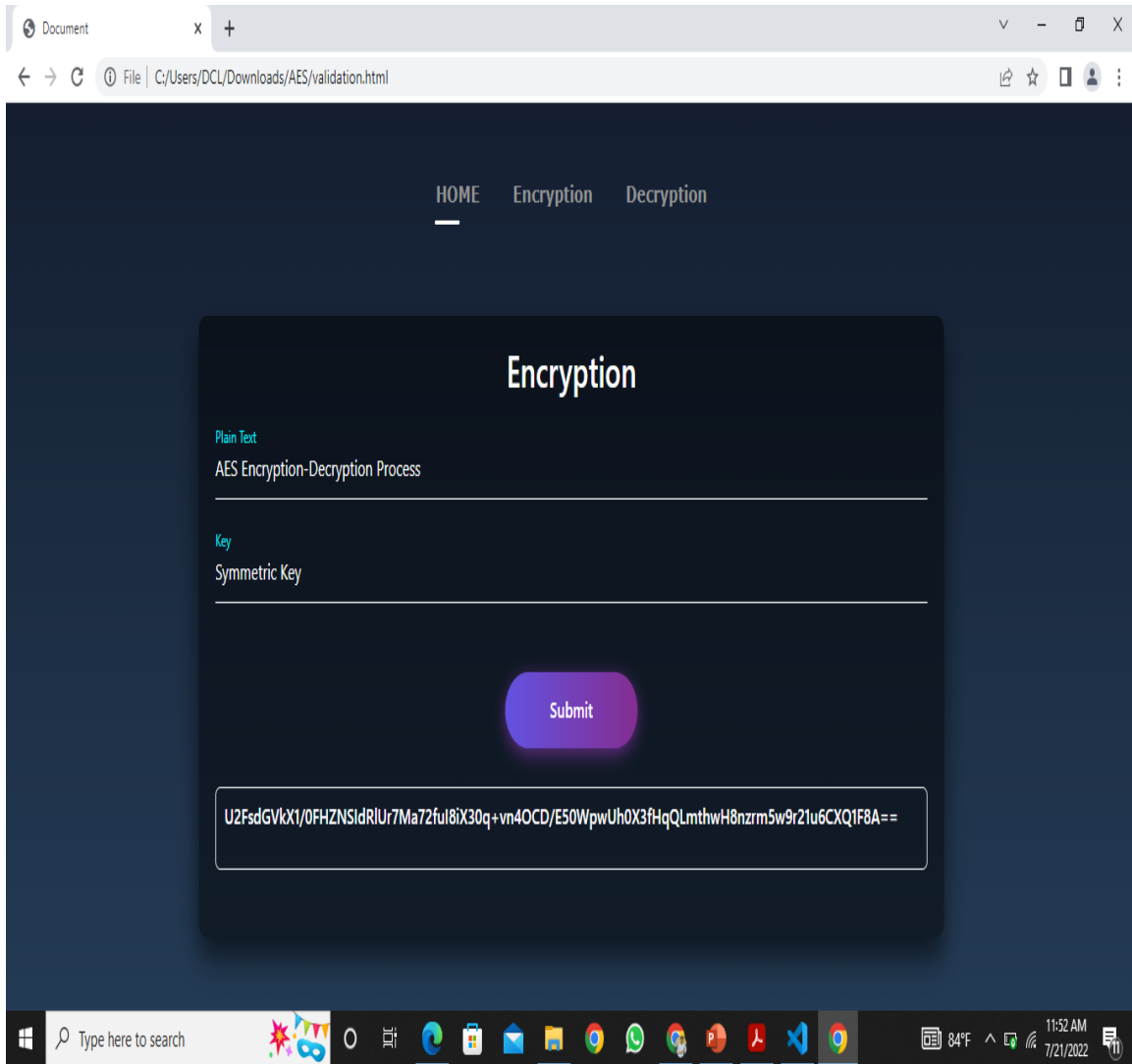


Figure 4.1: Output of Encryption Process

The encrypted text was used for decryption, and the receiving end need to change the cipher text. Hence, for decryption at first, used cipher text which gets from the sender ends and used the same secret key that was used for encryption. After completing the process, the decryption system returns the original plain text “AES Encryption-Decryption Process” to

the user. The receiver now can read the original message that the sender sends to his/her. In the following figure 4.2, we represent the result of the decryption process.

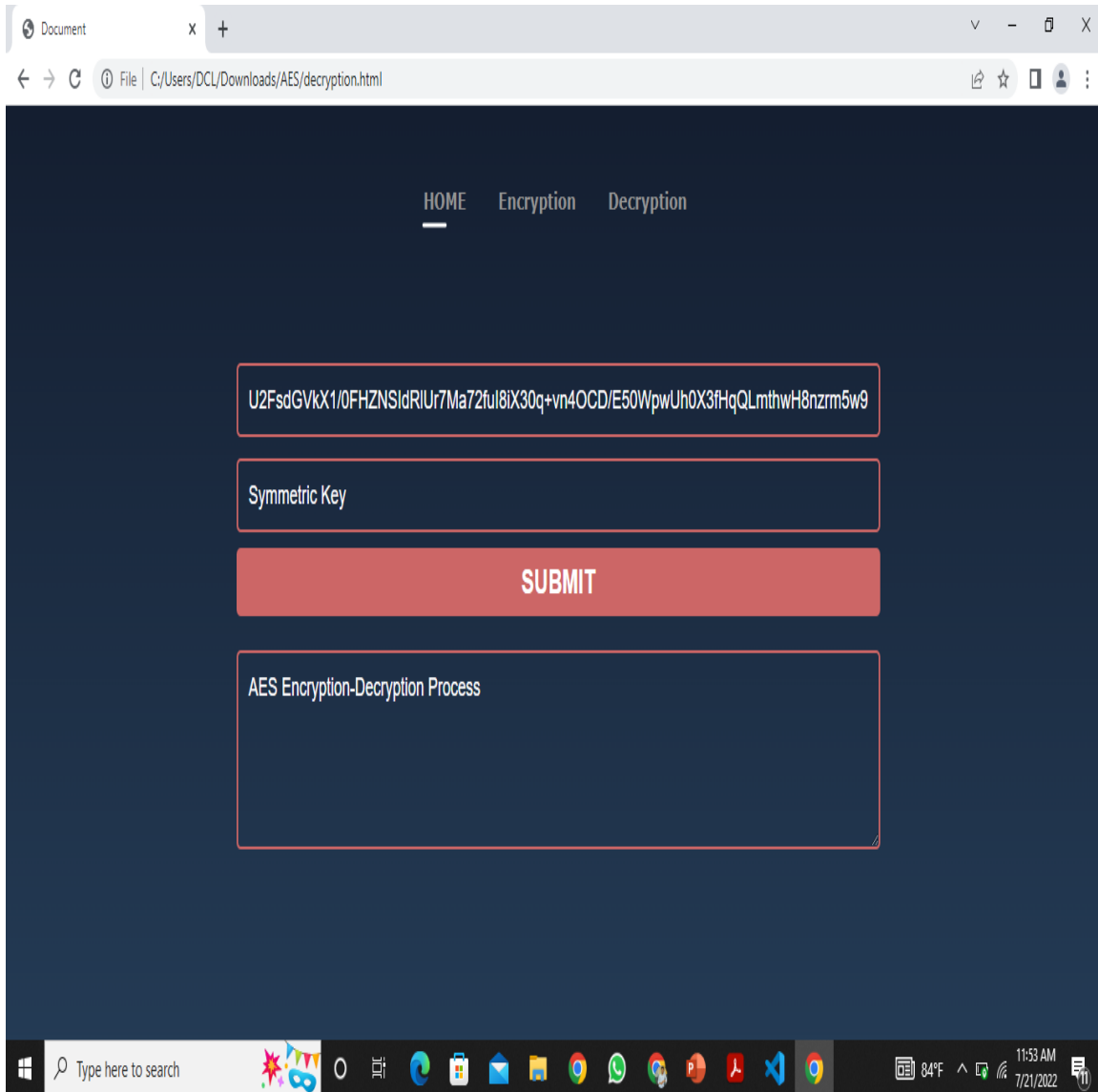


Figure 4.2: Output of Decryption Process

Although the text forms alter in the middle of the communication, the recipient still receives the exact message that was intended for him or her. This implies that thieves or hackers cannot correctly copy the text and move it between two users. Our suggested model can accurately guarantee data security.

Here, in the following table, we show some sample texts which we encrypt using the proposed model and the secret key used in the encryption and decryption process. Then generated cipher text by the encryption process. Table 4.2.1 shows the outcomes of the proposed model.

Table 4.1: Output of the model

Plaintext	Key	Ciphertext
How are you Mr. Alice?	EncryptionKey	U2FsdGVkX1+Lr22SwsqI1ixciay3VX3 tjyQZ4Jzgh2xPwqgpURoGD7TQlt2u1j6H
Send message to receiver	256-bit Key	U2FsdGVkX1+8wGic7yujal5zpJ5ois6W0B jZ5z32g+rn5eA4yUG8cYcxkj+yNRqU
Where are you come from Aysha?	AES Symmetric Key	U2FsdGVkX19kSxvzBMjxlTxRXWVfnRGP Y3AOEgVncNXyAa+RBEEn4uetqXetyvNH3
Decrypt cipher text to get original plain text	Secret key for decryption	U2FsdGVkX19Jv0rm/ZkxpamIDriV6wYF2N fe2RH2IyXuXbbuPzz7WDLjuaHQQAWJcybv NUDAm6z3iBQ7KGHMxA==
Secret message transfer system using AES	Secret Key for encryption	U2FsdGVkX1+VAP91vqFSZaLaCfRJThD R4iRRPieB62iTjp5KzRQJrEvoYUVgzYm Xn7gjMaoS4N7e2ErZ1qcqVg==
Encrypt message through secret channel	AES Secret Key 256-bit	U2FsdGVkX1++6FkWfhW5KoVaMu9Gzy xopPI0WOJ8LFvINANorbryt9vILYU2zF0e C9/ScLabzPiarAU2nfN8hQ==

### 4.3 Discussion

The initial aim of this study was to maximize data security and protect information from hackers. We specifically tested this proposed encryption mechanism on text messages. In this section, we discuss the key findings of this proposed model and the performance of the

algorithm. We used AES symmetric key algorithm for better performance. Our proposed model encrypts the message using the secret key which generates cipher text. Cipher text makes our model strong because it's impossible to read. The end user gets the original text without any interaction from the outside. Its key generation technique is too complicated which makes this model the strongest. However, our proposed model is limited to only short text messages but other kinds of messages like png, files, audio, and video can't encrypt. We can use this model on various platforms in the real world to ensure their security and its area will increase shortly when we can overcome our limitations. Finally, the accuracy of the proposed model is approximately a hundred percent and our finding indicates that the AES encryption process is much more accurate than others.

## **CHAPTER 5**

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

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

People today are concerned about their information security and how to prevent data stolen or keep hidden. Cryptographic encryption systems can solve this issue and prevent data insecurity. The impact of cryptography on society is significant and unbelievable. We want to ensure people's data security and provide a secure way for communication using the cryptographic method. Where people can transfer their information or store it online without any anxiety. Nowadays, people are feeling insecure to communicate with their friends and families due to the risk of data leakage and theft. Many people suffer from this and they lost their valuable data as well as in many cases it was a negative impact on relationships between people in society. Our proposed model removes this problem and provides a secure communication system because it is hard to crack. Because we used a strong key for encryption and decryption That's why intruders cannot see what people share with people online. In addition, our proposed model keeps hidden people's financial transaction data and credit card data due to this type of data being extremely sensible for the user. If hackers got this data from any source, they can theft user money, so people can prevent this unusual circumstance. Sometimes people share some sensible or secret data with friends or relatives which will be dangerous if it will publish but this model provides secure transactions. People in the future can easily communicate with other people without risk and can share confidential files or documents through secure communication methods.

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

Every technological innovation has a significant impact on the environment. Technology has both positive and negative effects on nature. Cryptography also has an impact on the environment and helps to save our earth. Data is the main source of every nuclear power

plant, oil production plant, hazardous gas base, and electric power plant. These plants stored their crucial data in a database or online and sometimes they transfer data for others working purposes. If any hackers and malicious attackers get this data, they can use this data for destruction. In recent years, many countries are victims of hacker attacks on their systems using the chance of insecure communication channels and weak systems. Third parties can do any serious occurrence using this data. The whole world will suffer from this and the ruins of the environment will be unbelievable. Because these plants contain highly explosive and dangerous chemicals for the earth. The air, water, and soil will be polluted and dangerous for humans and animals. If the system of these plants fails for data theft or malicious attack, it could be serious for people and the environment. So, our main purpose is to secure data and communication. They can pass their important data secretly to other ends and hackers cannot find what they send. Moreover, authorities store keys and passwords which are confidential and need to ensure security. The cryptographic method can change this scenario due to the strong encryption process. So, we can assure high-performance and advanced communication methods for information and reduce the environmental threat as well as can save our earth from some disaster. For this, necessary to enhance the security of some sensitive plants' data and use the cryptographic method.

### **5.3 Ethical Aspects**

Ethical issues are included in every sector and technological development. When doing something new at the same time comes with ethical aspects. Ethics is also included in the cryptographic- encryption, and decryption process. Cryptography is one of the most recent technologies to be confronted with several universal legal and ethical challenges relating to information security. The rising use of cryptographic technologies has highlighted several ethical concerns around the world, many of which are directly tied to fundamental human rights. That's why need to avoid ethical issues when ensuring data security and assuring user identity. In a secure communication system necessary to consider some ethical aspects like privacy issues, trust of users, reducing people's concerns, freedom of information dimensions, and respect for the privacy of others.

- **Privacy issues:** Cryptography assures data security, data integrity, and confidentiality as well as hidden user information. Who sends the data to other ends and who receives it needs to keep it secret. This is every person's right to secure their communication.
- **Prevent unauthorized access:** The unauthorized users are a major threat to security and they try to access data without permission. We should prevent and stop intruders to access communication.
- **Reduces user concern:** People are most of the time concerned about their valuable information security and our responsibility is to remove their anxiety.
- **Respect for other privacy:** Respect the user's personal information and do not interfere in their transactions. Just ensure secure communication and data security but what people's transactions should be their issues.
- **Freedom of information aspects:** People can transfer their data independently other people cannot interfere there. Sometimes the government tries to access residents' data for monitoring but people have the power to keep their information secret.

## 5.4 Sustainability Plan

Cryptography can provide long-term data security and safe data from hackers. Its security system is difficult to break easily due to the complex encryption process. Using a cryptographic system, we enhance data confidentiality and can keep it secret. Increasing the high-performance secret communication system needs more development and experimentation in various applications and data. Cryptography is a method used to secure all types of information or platforms like embedded data, cloud data, the Internet of Things (IoT), cryptocurrency data, and financial transaction data. Nowadays, every technological field uses a vast amount of data and this data are important for individuals and organizations. That's why authorities need to ensure data security that is possible using cryptographic security methods. In every sector, necessary to implement this method for long-term security purposes. For this reason, we want to use this model to secure different types of data like audio, video, image, pdf, etc. This model will be strong shortly because

try to increase its security complexity, so the model will be uncrackable and impossible to break. As a result, the platforms that used this model are their communication channel will be stronger. It would be the better approach for electronic data transactions. If we can implement this proposed system in real-life applications, then its efficiency can measure. Hence, we should focus on a wide range of applications and ensure their security properly. We are planning to develop a mobile application that protects users all data from hackers and sends notifications if find any risk. More advancement for the model need more study and funding required.



## CHAPTER 6

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

#### 6.1 Summary of the Study

Our primary goal was to establish a secure communication channel and ensure secure data transfer. We choose cryptography as the strong adversary method for communication security. We used our proposed model for message encryption which we use in daily life. We set random text and a secret key for encryption that produce cipher text. Then cipher text and the same secret key are used for the decryption process. This process converts our plain text into cipher text and again transforms it into plain text. We used the AES algorithm because it provides a higher level of data security. It is impossible to crack AES protection for intruders which makes our proposed system the strongest. The proposed model reduces the concern for information confidentiality and confirms effective data communication methods for users. It will be effective for various types of applications and increase people's information security.

#### 6.2 Conclusions

Currently, the advance in technology makes our life easier, and the involvement of people with technology has risen. At the same time, data security and data control have now under threat. Throughout this work, we tried to increase data security and control unwanted information theft. We applied the strongest AES algorithm for better performance. There is no evidence that intruders break the AES keys and find any weaknesses. This work prevents unauthorized access to the communication channel and makes the transaction secure. People can communicate with other people without any risk and they can transfer valuable information, and messages with family and friends.

### **6.3 Implication of Further Study**

Data security is a vast area for implications and is becoming more and more crucial as time goes on. People are looking for safe data-transfer solutions that use secure transactions. With time, people become more reliant on numerous programs and engaged online. As a result, data security drastically declines, and users lose control. That's why we want to develop our proposed model widely and expand its application area. Now we can encrypt text messages but we are planning to add another format of data such as audio, video, pdf, images, and files. Furthermore, we want to implement our proposed model in software systems and web applications to secure software and web data. Moreover, advanced and further study requires to development of the proposed model and needs to experiment with other algorithms.

## References:

- [1]. F.J. Kherad, M.V. Malakooti, H.R. Naji, P. Haghghat, "A New Symmetric Cryptographic Algorithm to Secure E-commerce Transaction." International Conference on Financial Theory and Engineering, IEEE, pp. 234-237, 2010.
- [2]. A. Anand, A. Raj, R. Kohli, Dr.V. Bibhu, "Proposed Symmetric Key Cryptography Algorithm for Data Security." 1st International Conference on Innovation and Challenges in Cyber Security, pp. 159-162, 2016.
- [3]. R.S.S. Kumar, T.P. Anithaashri, "Enhancement of Cloud Data Search Using Symmetric-Key Based Verification."
- [4]. A. Murtaza, S.J.H. Pirzada, L. Jianwei. "A New Symmetric Key Encryption Algorithm with Higher Performance". International Conference on Computing, Mathematics and Engineering Technologies, 2019.
- [5]. C-Chung. Lu, S-Yin. Tseng, "Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter." IEEE International Conference on Application-Specific Systems, Architectures, and Processors, IEEE, 2002.
- [6]. R. Jain, R. Jejurkar, S. Chopade, S. Vaidya, M. Sanap, "AES Algorithm Using 512 Bit Key Implementation for Secure Communication." International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, pp. 3516-3522, March 2014.
- [7]. J. Yenuguvanilanka, O. Elkeelany, "Performance Evaluation of Hardware Models of Advanced Encryption Standard (AES) Algorithm." IEEE SoutheastCon, pp. 222-225, 2008.
- [8]. R. Rayarikar, S. Upadhyay, P. Pimpale, "SMS Encryption using AES Algorithm on Android." International Journal of Computer Applications, Volume 50– No.19, pp. 12-17, 2012
- [9]. M.O. Onyesolu, N.O. Ogwara, "ON INFORMATION SECURITY USING A HYBRID CRYPTOGRAPHIC MODEL." International Research Journal of Computer Science (IRJCS), Vol. 4 (11), pp. 15-22, 2017.
- [10]. M. Biglari, E. Qasemi, B. Pourmohseni, "Maestro: A High-Performance AES Encryption/Decryption System." IEEE, pp. 145-148, 2013.
- [11]. Sindhuja K, P. Devi S. "A Symmetric Key Encryption Technique Using Genetic Algorithm". International Journal of Computer Science and Information Technologies, vol. 5 (1), pp. 414-416, 2014.
- [12]. N.G. BARDIS, K. NTAIKOS, "Design of a Secure Chat Application based on AES Cryptographic Algorithm and Key Management." Mathematical Methods, Computational Techniques, Non-Linear Systems, Intelligent Systems, pp. 486-491, 2008.
- [13]. V. Shokeen, N. Yadav, "Encryption and Decryption Technique for Message Communication." International Journal of Electronics & Communication Technology, vol. 2, issue 2, pp. 80-83, 2011.
- [14]. S. Radhika, A.C Sekar, "AES Algorithm Using 512 Bit Key Implemented for Secure Communication." Global Journal of Computer Science and Technology, vol. 10, issue 13, pp. 2-5, 2010
- [15]. M. BAYKARA, R. DAS, G. TUNA, "A Novel Symmetric Encryption Algorithm and its Implementation." Turkish Journal of Science & Technology, vol. 12 (1), pp. 5-9, 2017.

[16]. S. AN, Ms. Aruna, "Cloud Security Architecture Based on User Authentication and Symmetric Key Cryptography Techniques."

[17]. R. Padate, A. Patel, "Encryption and Decryption of Text using AES Algorithm." International Journal of Emerging Technology and Advanced Engineering, vol 4, issue 5, 2014.

[18]. S. Ariffin, R. Mahmud, R. Rahmat, N.A. Idris "SMS Encryption using 3D-AES Block Cipher on Android Message Application." International Conference on Advanced Computer Science Applications and Technologies, 2013.

[19]. J. Yenuguvanilanka, O. Elkeelany "Performance Evaluation of Hardware Models of Advanced Encryption Standard (AES) Algorithm." IEEE SoutheastCon, 2008.

## AN AES ALGORITHM-BASED SECURED SHORT-MESSAGE TRANSACTION

### ORIGINALITY REPORT

<b>16%</b> SIMILARITY INDEX	<b>11%</b> INTERNET SOURCES	<b>7%</b> PUBLICATIONS	<b>4%</b> STUDENT PAPERS
--------------------------------	--------------------------------	---------------------------	-----------------------------

### PRIMARY SOURCES

<b>1</b>	<a href="https://dspace.daffodilvarsity.edu.bd:8080">dspace.daffodilvarsity.edu.bd:8080</a> Internet Source	<b>2%</b>
<b>2</b>	Abhishek Anand, Abhishek Raj, Rashi Kohli, Vimal Bibhu. "Proposed symmetric key cryptography algorithm for data security", 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 Publication	<b>2%</b>
<b>3</b>	Fahime Javdan Kherad, Hamid R. Naji, Mohammad V. Malakooti, Payman Haghghat. "A new symmetric cryptography algorithm to secure e-commerce transactions", 2010 International Conference on Financial Theory and Engineering, 2010 Publication	<b>1%</b>
<b>4</b>	<a href="http://fbe.firat.edu.tr">fbe.firat.edu.tr</a> Internet Source	<b>1%</b>
<b>5</b>	<a href="http://www.ijarcs.info">www.ijarcs.info</a> Internet Source	<b>1%</b>