SECURING FILE SHARING USING AES-CBC AUTHENTICATED ENCRYPTION

Chan Myae Thu

M.C.Sc. **September 2022**

SECURING FILE SHARING USING AES-CBC AUTHENTICATED ENCRYPTION

By

Chan Myae Thu

B.C.Sc.

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Computer Science

(M.C.Sc.)

University of Computer Studies, Yangon

September 2022

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my sincere thanks to those who helped me with various aspects of conducting research and writing this thesis. To complete this thesis, many things are needed like my hard work as well as the supporting of many people.

First and foremost, I would like to express my deepest gratitude and my thanks to Prof. Dr. Mie Mie Khin, Rector of the University of Computer Studies, Yangon, for her kind permission to submit this thesis.

My heartfelt thanks and respect go to Prof. Dr. Thandar Win, Principal and Pro-rector of the University of Computer Studies (Myeik), for her invaluable and administrative support.

I would like to express my appreciation to Prof. Dr. Si Si Mar Win, Professor, Course Coordinator, M.C.Sc.(Thesis), Faculty of Computer Science, University of Computer Studies, Yangon, for her superior suggestion, administrative supports and encouragement during my academic study.

I would like to express my respectful gratitude to Prof. Dr. Tin Zar Thaw, Professor, Course Coordinator, M.C.Sc.(Thesis), Faculty of Computer Science, University of Computer Studies, Yangon, for her superior suggestion, administrative supports and encouragement during my academic study.

My thanks and regards go to my supervisor, Prof. Dr. Amy Tun**,** Professor, Head of Faculty of Computer Systems and Technologies, University of Computer Studies, Yangon, for her support, guidance, supervision, patience and encouragement during the period of study towards completion of this thesis.

I also wish to express my deepest gratitude to Daw Hnin Yee Aung, Lecturer, Department of English, University of Computer Studies, Yangon, for her editing this thesis from the language point of view.

Moreover, I would like to extend my thanks to all my teachers who taught me throughout the master’s degree course and my friends for their cooperation.

I especially thank to my parents, all of my colleagues, and friends for their encouragement and help during my thesis.

ABSTRACT

Today people are widely used internet, electronic records because of their ease of alteration and fast transition. The society is becoming more and more digitalized – therefore Information security is becoming more important than ever. The need for everyone to identify themselves in a digital way has spawned a wide variety of challenges, such as, for example, how to avoid fraud. Data security is main topic while transferring data from one place to other for protection of data from unintended user. Cryptography is essential for data security. Data encryption is an easy means of securing personal or business data protection. Many secure transmission techniques require any encryption. In the proposed system, the encryption will be concurrently used AES-CBC in secure data sharing. For secure key sharing purpose, this system will also be used El-Gamal encryption algorithm to encrypt the AES-CBC's symmetric key.

Statement of Originality

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

……………………..
Date

…………………
Chan Myae Thu

CONTENTS

Page

ACKNOWLEDGEMENTS **i**

ABSTRACT **ii**

CONTENTS **iii**

LIST OF FIGURES **vi**

LIST OF TABLES **viii**

CHAPTER 1 INTRODUCTION **1**

1.1 Objectives of the Thesis 2

1.2 Related Work 2

1.3 Problem Statement 2

1.4 Organization of the Thesis 3

CHAPTER 2 BACKGROUND THEORY **4**

2.1 Information Security 4

2.2 Differing Perspectives 5

2.2.1 Individual Perspective 5

2.2.2 Business Perspective 5

2.2.3 Government Perspective 6

2.3 Assurance of Information Security 6

2.3.1 Confindentiality 7

2.3.2 Integrity 7

2.3.3 Availability 8

2.3.4 Authentication 8

2.3.5 Non Repudiation 8

2.4 Security Services 9

2.4.1 Access Control 9

2.5 Cryptology 9

2.5.1 Cryptography 10

2.5.1.1 Symmetric key algorithms 12

2.5.1.2 Asymmetric key algorithms 12

2.5.2 Cryptanalysis 13

2.5.2.1 Cipher Text Only Attack 14

2.5.2.2 Known Plain Text Attack 14

2.5.2.3 Chosen Plain Text Attack 14

2.5.2.4 Chosen Cipher Text Attack 15

2.5.2.5 Man In the Middle Attack 15

2.5.2.6 Side Channel Attack 15

2.5.2.7 Brute Force Attack 15

2.5.2.8 Birthday Attack 15

2.5.2.9 Linear Cryptanalysis 16

2.5.2.10 Differential Cryptanalysis 16

2.5.2.11 Algebraic Attacks 16

2.6 Cryptographic Attacks 16

2.6.1 Passive attacks 17

2.6.1.1 Snooping 17

2.6.1.2 Traffic Analysis 18

2.6.2 Active attacks 18

2.6.2.1 Masquerade 18

2.6.2.2 Replay 19

2.6.2.3 Modification 19

2.6.2.4 Denial of Service 20

2.7 Advanced Encryption Standard 20

CHAPTER 3 DIFFERENT MODES OF AES 22

3.1 Steps of AES Cryptographic Algorithm 22

3.2 Different Modes of AES 23

3.2.1 ECB Method of Activity 24

3.2.2 CBC Method of Activity 26

3.2.3 CFB Method of Activity 27

3.2.4 OFB Method of Activity 28

3.2.5 CTR Method of Activity 30

CHAPTER 4 SYSTEM DESIGN AND IMPLEMENTATION 33

4.1 Cipher Block Chaining (CBC) Mode 34
4.2 Initialization Vector (IV) 36
4.3 Secure Key Sharing 37
4.4 Implementaion of System 38
4.5 System Evaluation By Timestamp 49

CHAPTER 5 CONCLUSION, LIMITATIONS AND FURTHER EXTENSIONS 52

5.1 Limitations and Further Extensions 52

REFERENCES 53

PUBLICATION 55

LIST OF FIGURES

Figure	Description	Page
2.1	Assurance of Data Security	7
2.2	Security Services	9
2.3	Overview of Cryptology	10
2.4	Basic model of Cryptology	11
2.5	Symmetric Key Algorithm	12
2.6	Asymmetric Key Algorithm	13
2.7	Snooping Attack	17
2.8	Traffic Analysis Attack	18
2.9	Masquerade Attack	18
2.10	Replay Attack	19
2.11	Modification Attack	19
2.12	Denial of Service Attack	20
3.1	Scheme of the ECB mode of operation	25
3.2	Scheme of the CBC mode of operation	26
3.3	Scheme of the CFB mode of operation	28
3.4	Scheme of the OFB mode of operation	30
3.5	Scheme of the CTR mode of operation	32
4.1	AES algorithm grouping and encryption diagram	33
4.2.1	Encryption in the CBC Mode	35
4.2.2	Decryption in the CBC Mode	36

4.3 System Flow 39

4.4 User Register Login 40

4.5 User Login 40

4.6 Message Encryption By AES-CBC (For Document File) 41

4.7 AES-CBC Key Encryption by ElGamal 42

4.8 Message Encryption Need By AES-CBC Key 43

4.9 Message Encryption Need By ElGamal Key 44

4.10 Successful Message Encryption 45

4.11 Successful Message Decryption 46

4.12 Denied Message Decryption(For Excel File) 47

4.13 File List By AES-CBC 48

4.14 Database Design By AES-CBC 48

4.15 Time Consuming Monitoring(For Document File) 49

4.16 Encryption Time Consuming Monitoring (For Excel File) 49

4.17 Decryption Time Consuming Monitoring (For Excel File) 50

LIST OF TABLES

Table	Description	Page
4.1	Time Consuming Analysis Table (Encryption Time)	50
4.2	Time Consuming Analysis Table (Decryption Time)	51

CHAPTER 1

INTRODUCTION

Documents can be grouped into business and non-business, where noncommercial records can be moreover organized into secret and non-characterized (See Figure 1.1). Business and non-business anyway grouped records are sensitive which suggests that they ought to be protected from anticipated attacks or misuses. Such follows could provoke unapproved divulgence (Mystery attacks), unapproved change (Uprightness attacks), or unapproved keeping (Openness attacks). These different sorts of attacks can be performed on records while they are being moved, set aside, or used by either supported or unapproved clients. Consequently, protections for such attacks begin from three specific fields of wellbeing which are: Correspondence security which is stressed over hindering different sorts of attacks on data conveyed over an association; Line security which is stressed over preventing attacks on data set aside inside a trusted in inside association; and Insider security which is stressed over thwarting attacks on data by individuals who have been supported with access.

Nowadays a huge piece of the correspondence is done utilizing electronic media. Information Security expects the central part in as correspondence. In this manner, there is a need to shield information from harmful assaults. Cryptography is an assessment of secret codes, connecting with secret of correspondence through a questionable channel. It safeguards against unapproved parties by thwarting unapproved change of direction. Cryptographic computations are essential in data security where information is mixed at the transporter side and decoded at the recipient side. PC and correspondences structures use cryptography for three broad purposes — to defend the arrangement of information (i.e., encryption), to shield the trustworthiness of information, and to approve the originator or wellspring of information. A symmetric block figure, the General Encryption Standard (AES) estimation was adopted by NIST in 2001. AES block size is 128 bits, however the size of encryption key can be 128, 192 or 256 bits. Strategies for action may similarly give usage of the block figure on a surge of plaintext and make the estimation more useful. This proposed secure report sharing system will be executed by CBC method of AES encryption.

1.1 Objectives of the Thesis

The objectives of these thesis are:

- To safeguard a secrecy of advanced information put away on PC framework or sent by means of the web or other computer network
- To keep outsiders from recuperating any of the first information or even any data about the information, from scrambled information
- To show CBC mode of AES activity has boundaries which require cautious and right determination and execution
- To explore an operation of CBC mode on AES for .doc and .xlsx file encryption

1.2 Related Works

In this study the usage of AES as a record security structure is finished, where the encryption and translating process is finished on the report. In testing the structure a primer is performed on all reports with different record sizes and for the outcomes of the encryption cycle (figure text) as records with the record plan with the *.encrypted extension [1].

[2]This structure bases on the productive examination of these issues and summarizes AES estimation execution, complete application and computation assessment with other existing strategies. To separate the introduction of the proposed computation and to make the most of the potential gains of AES encryption estimation, one necessities to reduce round key and work on the key plan, as well as normally coordinate with RSA estimation. The encryption system uniting AES and RSA estimation exploits the advantages of symmetric key and astray key. The gathering key used in the archive is mixed by RSA, and the encryption of data record is encoded by AES.

1.3 Problem Statement

Nowadays, private data exposure has been happened unintentionally or deliberately in numerous associations. By inadvertently sending the classified data to unapproved individual who isn't from association could prompt a difficult issue or hazard. Message transmission through organization will confront numerous dangers like unapproved access and sneaking around. The aggressor may took or changes the substance of message during transmission. Utilizing the cryptography calculations before transmission can assist with decreasing the gamble. Accordingly, tied down informing is a significant issue to meet the objectives of cryptography, CIA (Confidentiality, Integrity, and Availability). To shield message from aggressor or unapproved individual, the first message should be scrambled to ensure it is unintelligible to anybody. The message just can be perused by the individual who has the exceptional key.

1.4 Organization of the Thesis

The thesis is coordinated in five parts. They are as per the following:

In Chapter 1, introduction of the system, objectives of the thesis, related works and thesis organization are described.

Chapter 2 presents the background theory.

Chapter 3 discusses the security controlling techniques

Chapter 4 expresses the design and implementation of the proposed system.

Finally, **Chapter 5** presents the conclusions, advantages of system and limitations and further extensions of the system.

CHAPTER 2

BACKGROUND THEORY

2.1 Information Security

For hundreds and centuries, sovereigns and furnished force leaders have trusted in on viable correspondence to control their nations and request their enormous militaries also, simultaneously, they have all had some significant awareness of the results of their message falling into a few unsuitable hands, uncovering important secrets to match nations and beguiling fundamental information to limiting powers. The bet of enemy catch pushed the early progression of cryptographic computations and methodologies to cover with the objective that principal the arranged recipient can figure out it. Data security can be suggested as the demonstration of protecting data from nonsensical permission, adjusting and the destruction. This moreover means to safeguard the security, reliability, openness of information, either away, taking care of or transmission. The fast progression of web and correspondence and communication channels have met the demand for better encryption techniques to protect privileged data associated with lawmaking bodies, military, crisis centers and private affiliation. Different attacks are being recorded everyday on government locales, got data vaults, one individual to the next correspondence destinations, email organizations and assessment workplaces all over the planet. A couple of supposed foundations and affiliations are persistently funding research associated with security and information affirmation with a common target to deal with impending risks associated with the security and steadfastness of data structures.

The terms PC security, data security and information affirmation are tradable and covers various frameworks used in both public and classified space, that being involved consistently for typical organizations as online monetary trades, web correspondence using messengers and different talk programming, versatile calls and VoIP clients. Additionally, openness of more humble, even more amazing and more reasonable figuring gear have made electronic data dealing with contraptions within the area of residential and commercial clients. Additionally, the field of cryptography has undergone enormous change since the turn of the twenty-first century and data security in light of huge use of advantageous devices like high level cells, tablets and GPS devices.

2.2 Differing Perspectives

Key security frameworks utilized in the most cutting-edge applications in the world are organized in systems that correspond to different electronic climate applications. It is what is really going on with current cryptography. Three alternate points of view have been distinguished that have assisted with forming the advanced utilization of cryptography in software engineering and information science.

2.2.1 Individual Perspective

Every person believes he has a fundamental right to shield his private information from adversaries. Someone from past classified space is the enemy, endeavoring to take the data. Along these lines, he uses different cryptography strategies to ensure that information stays baffling in vastly broadening public region. Along these lines, the perspective of load of individual clients is to include the purposes of cryptography under some condition for disguising their own data.

2.2.2 Business Perspective

Little to medium-sized businesses use a variety of open communication channels and PC networks and immense affiliations, rely upon web and one can't decide to ignore from the countless gifts that these associations and channels have introduced to by adjusting the essential strategies anyway they have also procured basic perils cover. Along these lines, for the business viewpoint, cryptography ought to be noticeable as the storage facility of gadgets used to give capable access control structures, information hiding away and dependability philosophy both encryption estimations and going probably as the establishment mainstays of business security and guaranteeing monetary result of the affiliation. This is absolutely a reality that the result of an affiliation depended totally based on the protection of its history and data is stacked with models that support this idea. In this manner, the main goal of cryptography for business is to raise security expectations without sacrificing the normative work.

2.2.3 Government Perspective

During the cutting-edge season of mechanical movement, states from one side of the planet to the next are endeavoring to check computerized bad behavior and advanced mental mistreatment due to a complex issue where cautious clients are taking extensive measures to cover the security to defend themselves from attackers, organizations from experts in the field of cryptography are being involved, which hence makes it challenging to examine the things in their transmission. Nevertheless, as per the public power's perspective such clients fall in the class of questionable clients and are consistently inconspicuous.

Differing perspectives unquestionably lead to likely hostile conditions between substitute perspectives.

- For example, a couple of lawmaking bodies have requested the security provider associations to quickly pass stipulations in cryptographic computations on to work with the most well-known approach to surveilling individuals, which hence is an encroachment of individual open door.

- Several state-run organizations have imposed strict rules limiting access, including restrictions on the public's right to monitor private correspondence between individuals and social gatherings. It is similarly suggested as the huge security break in the security of individuals and arrangements.

2.3 Assurance of Information Security

The fundamental principles of data security are confidentiality, integrity, and availability in Figure 2.1.

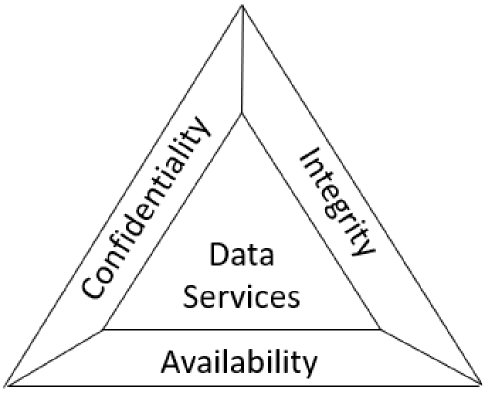


Figure 2.1 Assurance of Data Security

2.3.1 Confidentiality

Most of the time, classification and security are synonymous, and it implies the use of encryption techniques to ensure that only authorized clients can access the limited information and the confirmation of that information from unapproved clients. Approval techniques, accessing control the frameworks include check utilizing usernames and passwords guarantee that the secret information stays open just to the relegated client.

Further, a client must enter a one-time secret word completely finished his mobile phone connected with a username and a secret phrase in order to sign in and start an electronic transaction. This feature, known as two-way approval, is used by various email and banking organizations. Another option for concealment is to use security tokens and biometric devices during the affirmation process.

2.3.2 Integrity

Integrity makes sure that data isn't altered while in transit or altered by unauthorized clients. Let's imagine that someone starts a financial transaction to send their friend $500, but in the middle of it, a fraudster changes the amount to $5,000 and the recipient's name to his own, along with his own account number. The bank and the source may then have a bothersome problem.

The strategy for giving dependability is to utilize cryptographic checksums. This is made utilizing hashing computations, which are one-way ability (for instance irreversible capacities where the data cannot be made back from the outcome).

2.3.3 Availability

This alludes guarantee that data is accessible reliably when anticipated by certifiable clients. Information has' all's worth, right whenever supported clients access it at wonderful open doors. These days, software engineers frequently use DDoS attacks to crash the servers of targeted locations. In these attacks, the server continuously satisfies the attacker's requests but eventually becomes overloaded due to high sales, which causes the web server to crash and intrude on the organizations.

When a problem arises, availability calls for quick hardware tuning and maintenance. Security features include automatic detection of harmful requests and unquestionable level hardware (such as using multiple hard drives to store data). Strikes are used to provide openness.

2.3.4 Authentication

Evidence recognition is ensured by authentication. To determine if someone is truly as unique as they have claimed to be, a framework is used. The approval process includes multiple character confirmations, such as something the real client knows (like a secret key), something he has (like a real device, like a person card or charge card), and something he is (for instance finger impression or iris).

Even though one of these checks is sufficient in the vast majority of situations, there are some security fundamental structures used in nuclear power plants and where public safety is a concern (for example, the military) that call for the affirmations to unquestionably be used in synchrony with one another to ensure the highest level of security while approval.

2.3.5 Non repudiation

It makes sure that the social gatherings attracted by an online trade cannot deny receiving a compelling trade or ever having started the trade. It is the capacity to demonstrate that an event occurred at a specific moment. The absence of non-revocation can lead to problematic problems. Imagine a scenario in which the recipient of a bank transaction claims that he did not receive the optimal amount of money and the transporter is unprepared to certify the transaction's successful completion.

The use of cutting-edge marks is integrated into the security component for non-repudiation. These imprints prove that the message was sent by the designated client because they painstakingly sign a document using the transporter's secret key.

2.4 Security Services

The five security services that the International Telecommunication Union-Telecommunication Standardization has defined as shown in Figure 2.8.

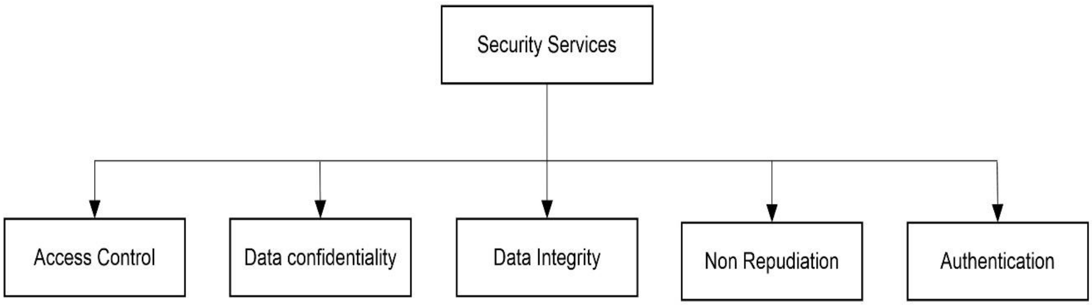


Figure 2.2 Security Services

2.4.1 Access Control

Access control is capable of praising various types of reliable clients who are employed by an association or on a clear-cut system. According to the task of a person, this framework can grant or modify assents related to read, create, and eradicate a specific record. Access control, which can be implemented with the aid of usernames and biometric devices, is occasionally additionally recommended as a clear barrier to resource induction.

2.5 Cryptology

Science's branch of cryptology oversees the study of creating or settling codes and codes. It is a combination of mathematics and arithmetic, and it is further divided into the two broad classifications of cryptography and cryptanalysis.

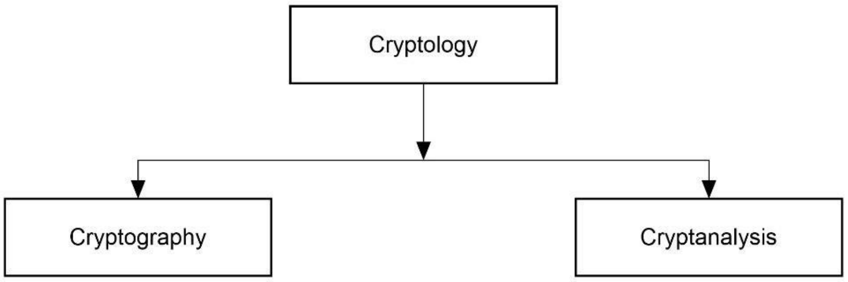


Figure 2.3 Overview of Cryptology

2.5.1 Cryptography

Greek words "kryptós," which mean hidden or secret, and "graphein," which means making, are the roots of cryptography. It is an example of secret writing that is used to communicate sensitive information over open gatherings. In this type of writing, things in an extraordinary message are transformed into distorted structures that can only be recovered by the designated person. Around 1900 BC, cryptography was being used in antiquated Egypt, where various pictographs had been cut up for entertainment and enigma. Julius Ceaser first used cryptography as a baffling method for correspondence between the years 100 BC and 40 BC to conceal important information. His code became the cornerstone of modern cryptography and is referred to as the "Ceaser Code," where each Roman letter is moved by three circumstances apart.

Early encryption schemes were very transparent and included basic mathematical operations to completely convert plain text to encoded text. These techniques were completely ineffective against repeated attacks. Since they were used so extensively in the transmission of sensitive information starting at the start of the Second Great War, cryptographic estimates have grown more muddled with each passing day. Additionally, the use of PC systems has complicated the field of healthcare because modern techniques perform encryption and unscrambling extremely quickly, and that too at the cycle level. Additionally, modern cryptography is based on explicit mathematical conditions that are extremely difficult to resolve unless a few unique conditions are met. Because of these characteristics, it is incredibly difficult and tenacious for a person to crack modern cryptography.

A sender using an encryption algorithm to hide some sensitive data before sending it to the intended recipient. While doing so, the attacker tries to intercept the message and decrypt it as shown in Figure 2.4.

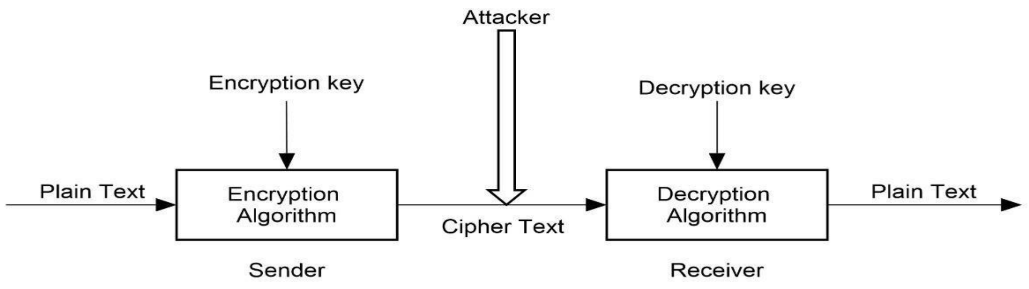


Figure 2.4 Basic model of Cryptography

Different elements of the model are described below:

- Plain message is the characterized information that will be mixed and send over the association.
- Figure text is confidential information that has been combined with plain text using an encryption estimate.
- The estimation of encryption is a combination of astounding mathematical abilities that is used to scramble the confidential information.
- Estimation decoding also combines a variety of multifaceted mathematical skills that are used to decipher the confidential data. Unraveling estimates are typically regressive computations for encryption.
- The transporter uses the encryption key, a secret information, as one of the responsibilities to the encryption estimation associated with plain text to deliver a code text.
- The beneficiary uses an unreadable key as one of the commitments in the translation of estimate into figure text in order to obtain plain text.
- An aggressor is a substance that typically makes an effort to wait patiently while blocking the code text on the communication channel and attempting to convert the code text entirely to plain text.

In general, cryptography is divided into two categories: symmetric key assessments and incorrect key calculations. The mystery key used in symmetric key calculations has a specific encryption and translation goal. However, lopsided key calculations use a public/private key pair for encryption and unwinding.

2.5.1.1 Symmetric key algorithms

The sender encrypts a plain text using an encryption calculation and a typical mystery key as shown in Figure 2.5. The receiver decodes the code text on the opposing side by using the opposite of that encryption calculation (for example decoding calculation).

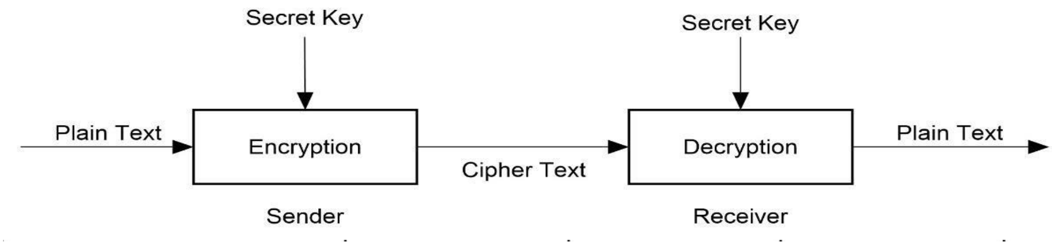


Figure 2.5 Symmetric Key Algorithm

The use of symmetric key calculations dates back to earlier times, but there is a problem with how the secret key is shared between the sender and the receiver. Furthermore, symmetric key calculations are more appropriate for scrambling huge amounts of data and are frequently very quick in contrast to uneven key calculations, which typically carry out focused mathematical operations. AES, DES, 3DES, SERPENT, MARS, CAST, RC6, TWOFISH, and IDEA are the estimations of secret keys that are most frequently used.

2.5.1.2 Asymmetric key algorithms

Figure 2.6 illustrates how asymmetric key calculations, which are used to encrypt and decrypt data, use two different keys. The source uses his confidential key to encrypt plain text, and the collector uses his public key to decrypt the coded text. Regardless of whether the adversary is aware of one of the two keys, it is challenging to reason with either a private or public key.

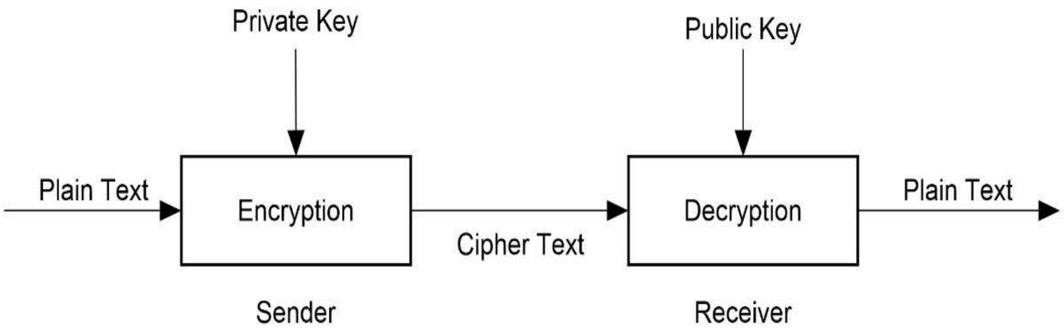


Figure 2.6 Asymmetric Key Algorithm

Utilizing asymmetric key computations has some drawbacks, including the requirement for key organization structures. Additionally, in order to be protected from attacks, every correspondence needs a different game plan of public and private key matches. The most frequent use of lopsided key computations is to alter a small portion of the data. RSA, ElGamal, and ECC are a few examples of asymmetric key computations. These estimates are typically slower than symmetric key computations when viewed differently, but they are most frequently used to use automated marks.

2.5.2 Cryptanalysis

In order to understand how cryptographic computations work and identify any flaws that could make them vulnerable, cryptanalysis involves surveying and evaluating them in a practical way. Military and some perception exercises supported by strong ties use cryptanalysis to test security-related fundamental systems. Additionally, programmers use cryptanalysis to exploit flaws in various systems and destinations. The most popular method of performing cryptanalysis isn't really necessary; it requires mathematical prowess and a thorough understanding of how encryption computations actually function. In the past, cryptanalysis was merely expected to solve the fundamental problem of deciphering a message; however, modern cryptography uses math and extremely fast computers to break an encryption computation. A typical cryptanalytic attack follows these four basic steps:

- Determine the language being used
- Determine the system being used

- Reconstruct the system
- Reconstruction of the plain text

It is essential to understand the type of language used as plain text and code text (for example, english, German, or French) in order to identify a flaw in a cryptographic computation. It can take some time to finish the system. This connection includes character repetition counting, looking for repeated models, and running quantifiable tests. While system expansion happens with the most popular method for discovering a secret key that has been used with the ultimate goal of encryption and it functions in agreement with the amusement of plain text. Cryptographic attacks depend on the type of information that is available and the estimation of the encryption. There are 11 different categories of cryptographic attacks in general. Each of them is asked for in the segments that follow.

2.5.2.1 Cipher Text only Attack

In this kind of attack, the attacker uses the language and information from the figure text to try to decode the encryption calculation. Recurrence analysis can be used to mount an attack, and occasionally the attacker isn't even aware of the encryption calculation that was used to achieve encryption.

2.5.2.2 Known Plain Text Attack

The attacker in this type of attack has access to both the plain text and the corresponding code text, and attempts to decipher the secret code or code book used in the encryption method. It addresses the need for the attacker to be aware of a known word that the source uses at a specific point in each message. A typical attacker is aware of the result that a specific piece of plain text will yield given its circumstances. In this way, rather than the entire message being cracked, assuming he creates a key that transforms the rehashed plain message into that specific code message. The partners adopted the same strategy.

2.5.2.3 Chosen Plain Text Attack

In this kind of attack, the attacker has access to both the plain text and the corresponding code text, and he is trying to figure out the secret code or code book that was used in the encryption method. It deals with the requirement that the attacker be aware of a known word that the source uses at a particular point in each message. An average attacker knows what will happen when a certain piece of plain text is used in a certain situation. In this manner, assuming he develops a key that converts the rehashed plain message into that particular code message, rather than the entire message being cracked. The partners used the identical approach.

2.5.2.4 Chosen Cipher Text Attack

In this type of attack, the attacker can pick different altered figure texts created from the first code text and are decode those code texts under the obscure mystery key to produce gauge about the mystery key. This sort of assaults is applied exclusively to Uneven key calculations.

2.5.2.5 Man in the Middle Attack

Open key calculations frequently use man-in-the-middle attacks. The aggressor typically stands between two imparting groups and arranges his own important trades with the two of them. Source and recipient communicate while acting as though they are using a reliable channel, but the aggressor reads every message that is being sent by them. Hashing and computerized signature calculation can be used to prevent this kind of attack.

2.5.2.6 Side Channel Attack

The performance of an encryption calculation is required for side channel attacks instead of real calculation like running season of a calculation, framework use during encryption and emanation of radiation. This sort of assault isn't over the top expensive to utilize and utilizes known figure text.

2.5.2.7 Brute Force Attack

A bruteforce attack involves trying every key that could possibly exist in order to generate a significant plain text. One of the most experienced and tiresome assaults. Let's assume that a 128-bit key is used in a symmetric key encryption calculation. In the worst case scenario, it would then take 2128 key blends to successfully crack it. The available computational power is absolutely necessary for this attack to be successful.

2.5.2.8 Birthday Attack

It is a brute force attack used solely to undermine hashing algorithms. According to the rule that in a gathering of 23 individuals, there is a half likelihood that two people have birthday celebrations around the same time and that likelihood floods to close to 100% in the gathering of 60 individuals. As hashing calculations are powerless to impact (two plain texts, for instance, can lead to the same hash), yet It is extremely difficult to find an impact in the contemporary hashing calculations as a result of bigger space. Along these lines, they can oppose this sort of assaults.

2.5.2.9 Linear Cryptanalysis

It is only used with block figures and is dependent on known plain text. It uses simple approximations to understand how a block figure behaves. With enough plain text and code text matches, the attacker can produce the mystery key. Straight cryptanalysis consists of two parts, the first of which is responsible for producing direct conditions related to plain text, the secret key, and code text, and the second of which uses the plain text and code text already known in the first part's direct conditions to produce the secret key.

2.5.2.10 Differential Cryptanalysis

It is used to hunt for block figures, stream figures, as well as on hashing calculations. It is also a type of picked plain text. The distinctions between the code texts produced by the two plain texts are what determine this type of assaults. In essence, it determines the portion of an encryption calculation that is not acting in a haphazard manner and uses this disadvantage as a driving force to produce the mystery key.

2.5.2.11 Algebraic Attacks

This classification of assaults relies upon the logarithmic construction of a calculation. As the vast majority of the block figures show serious level of numerical construction, an aggressor takes advantage of this thought to communicates the code activities into logarithmic conditions and substitute a known qualities into those situations to get the mystery key.

2.6 Cryptographic Attacks

Cryptographic attacks are the strategies used by an adversary to compromise a secured system. These attacks can be divided into two main groups.

- Passive attacks

- Active attacks

2.6.1 Passive attacks

In passive attacks, an intruder tries to focus on the relationship between the associations in order to learn some information and tries to break the system while taking into account the bundles that are split between source and recipient. Finding acknowledged plain texts is an instance of a disconnected attack in which an adversary examines the decoded traffic in search of private data such as usernames or passwords that have been spread across bestowing social occasions. The only justification for why uninvolved attacks are by far the majority covert is that they are unambiguously intended to harm the source and recipient while the system remains intact. For communicational purposes, encryption should be used extensively to protect any opportunity from discrete attacks like snooping.

2.6.1.1 Snooping

Snooping is a method of gaining unauthorized access to private information about a person or a relationship. By using specifically designed programming to secure remote access, sneaking around increases the likelihood of an attacker seeing the messages sent or received by a specific person or by detecting the presence of a body approaching his structure in the steady. The most frequently used and complex tools for skulking around are key loggers. The greatness of these key loggers is their capacity to operate in an impalpable mode, which prevents the victim from being aware of a security breach. They record every keystroke that has been pushed on the control center.

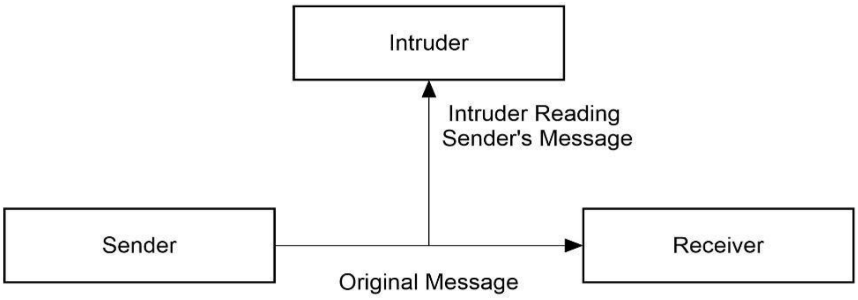


Figure 2.7 Snooping Attack

2.6.1.2 Traffic Analysis

As the name implies, it is a method of gathering and removing a lot of information from traffic packages that are sent over a network between a transporter and a gatherer. Clients who participated in the correspondence are unaware that an attacker is listening in on their correspondence lines.

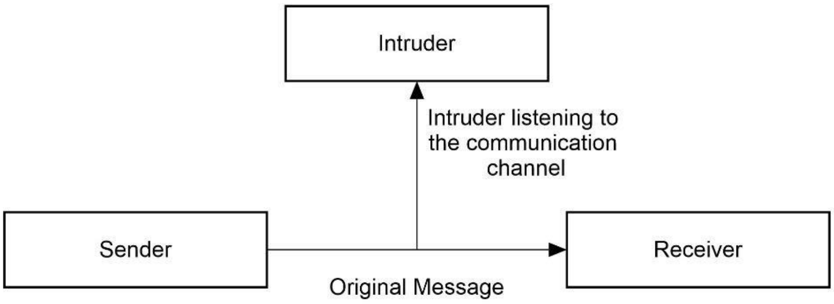


Figure 2.8 Traffic Analysis Attack

It can also be used to sort out a few important models in correspondence when the messages being transmitted are also encoded. Additionally, traffic analysis can reveal characterized data like IP addresses and Macintosh regions of the source and authority. These addresses are also used to determine the location of their property. The successful cryptanalysis of Mystery machine, which was used by Germans for correspondence during World War II, was one of the most astounding instances of traffic assessment.

2.6.2 Active attacks

In dynamic attacks, a trespasser tries to manipulate the information being sent over an association or inside a building to corrupt a PC using Infection, Trojan horses or worms. Dynamic attacks can be successfully perceived, actually yet are difficult to thwart in light of the fact that bona fide client have no impact over their own structure while getting through a surge. Four classes of dynamic attacks are Disguise, Replay, Adjustment, and Denial of Service.

2.6.2.1.1 Masquerade

In order to gain unauthorized access or higher status, an attacker poses as the legitimate client. It is possible to use camouflage by speculating on usernames and passwords or by identifying security loopholes in a system. Due to this attack, banks and other online retailers were forced to notify their customers and give them a reasonable amount of time to change their passwords.

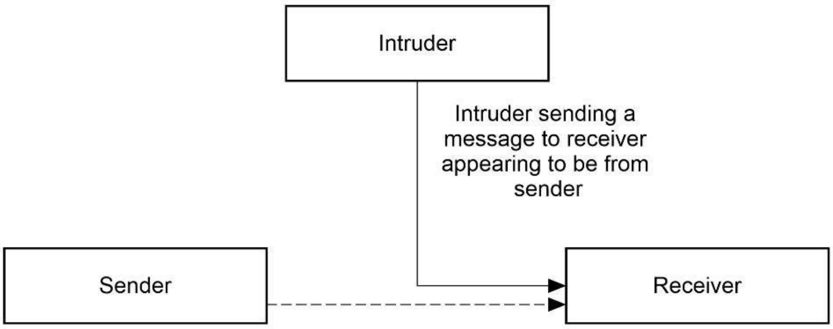

Intruder
Intruder sending a message to receiver appearing to be from sender
Sender
Receiver

Figure 2.9 Masquerade Attack

2.6.2.2 Replay

In this attack, the developer intercepts a message, stores it locally on its own computer, and then sends a similar message to the designated recipient once more. It might be successfully demonstrated with a model in which a person asks his bank to transfer a certain amount of money to one of his sidekicks, and the aggressor receives that request and sends it back to the bank later.

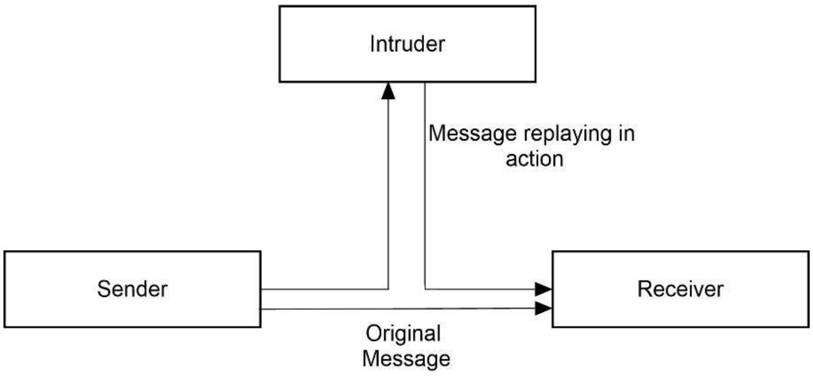


Figure 2.10 Replay Attack

2.6.2.3 Modification

Attacker changes the genuine things in a remarkable mandate to obtain individual benefit. Adjusted message can in like manner be used at the same time with replay attack. Moreover, interloper can in like manner change the message headers to reroute a comparable message to one more unbiased to hurt the main transporter. Allow us to anticipate what might happen if an administration employee receives a message from a pioneer from the battle zone referencing the sending of forts that has been changed to something else and directs the fight to a very unexpected side.

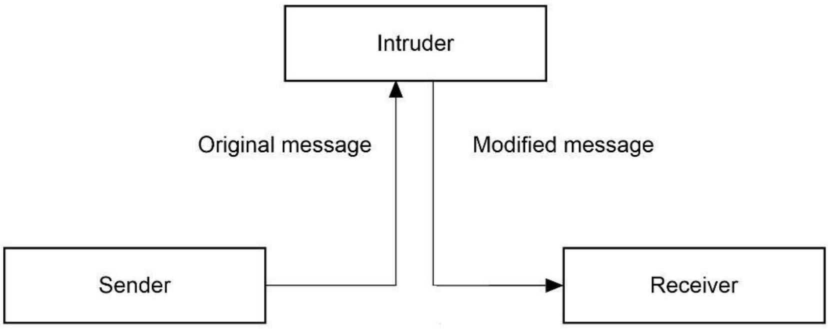


Figure 2.11 Modification Attack

2.6.2.4 Denial of Service

These attacks may temporarily suspend or completely shut down all services provided by a serious server. Attacker can overwhelm a web server by launching a large slide of company sales, which ultimately results in a crash.

A more sophisticated attacker can trick the tailored systems used to recognize Denial of Service attacks by rerouting the packages from currently corrupted machines.

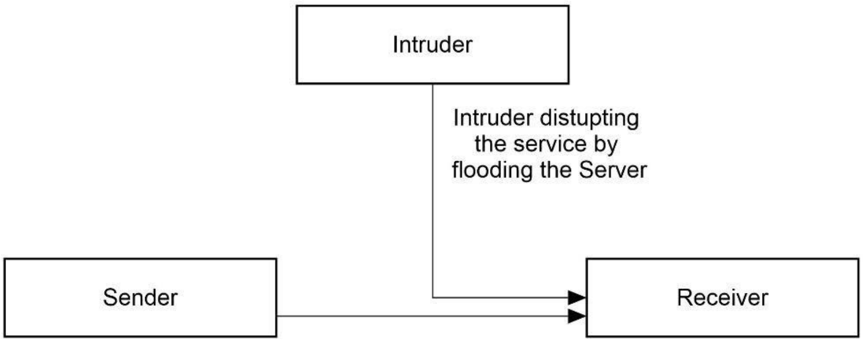


Figure 2.12 Denial of Service Attack

2.7 Advanced Encryption Standard

Advanced Encryption Standard (AES) was explicitly intended to supplant the maturing Information Encryption Standard, Its choice method started back in January 2, 1997 by National Institute of Standards and Technology (NIST) of the US of America [1] [2][3] when they brought world's best personalities in the area of cryptography to collaborate by introducing their thoughts for another encryption calculation to be called as Advanced Encryption Standard and prevailed in its plan with the accommodation of 15 calculations as possible contender for AES. NIST has additionally planned to make every one of the entries accessible to public for their significant remarks and surveys. The compulsory prerequisites for AES competitor entries were as per the following:

- Each block of AES ought to encode 128 cycle of plain text.
- AES ought to have the option to scramble the plain text utilizing any of the three key lengths (for example 128 bit, 192 piece or 256 cycle).
- It ought to be similarly productive in equipment as well as in programming.

After starting appraisals, five new calculations (MARS, RC6, Twofish, Snake, and Rijndael) have been chosen as AES finalists, following multitudinous audits and public examination, Government Data Handling Standard (FIPS) distributed the draft for Cutting edge Encryption Standard in February 28, 2001 and last AES was endorsed on November 26, 2001 as FIPS Bar 197 [2].

High level Encryption Standard (AES) officially known as Rijndael has a place with the group of Block Codes and was proposed by Joan Daemen and Vincent Rijmen [3]. It doesn't utilize Fiestel structure like Information Encryption Standard (DES) where 32 out of 64 bits are encoded in each round. All things considered, AES encode every one of the 128 pieces of plain text in a solitary round, which is the explanation of its lower number of rounds when contrasted with DES. Be that as it may, notwithstanding AES plan rules, genuine Rijndael calculation has the capacity to encode 192 or 256 bits of plain text.

CHAPTER 3

DIFFERENT MODES OF AES

The Advanced Encryption Standard (AES) algorithm utilizes the substitution permutation network as its foundation. Both in software and hardware, AES is quick. AES uses a 44 byte matrix known as a state to operate. The Advanced Encryption Standard cipher is described as a series of transformation sounds repeated so that the input plaintext is changed into the cipher text that is produced in the end. There are several processing steps in each round, one of which is dependent on the encryption key. Using the same encryption key, a series of reverse rounds are used to convert the cipher text back into the original plaintext.

AES encryption algorithm benefits:

- The Advanced Encryption Standard ensures security while also enhancing performance in a number of contexts, including hardware implementations, smartcards, and other settings.
- AES is a federal information processing standard, and no direct non-brute-force attacks have been made against it as of yet.
- AES is robust enough to be approved for use by the US government when encrypting top-secret data.

Alternative to Advanced Encryption Standard: SSl and TLS are two ciphers that can be used instead of Advanced Encryption Standard. Next to AES, RC4 encryption is used. RC4 has 128 bits. Fast cipher RC4 is constantly vulnerable to various kinds of attacks. Because of this, WEP wireless encryption performs poorly. As a result, AES is given precedence over other standards [15].

3.1 Steps of AES Cryptographic Algorithm

1. Key Expansion round keys are derived from the cipher key using Rijndael's key schedule.

2. Initial Round:

- Add Round Key each byte of the state is combined with the round key using bitwise xor.

3. Rounds:

- **Sub Bytes:** a non-linear substitution step where each byte is replaced with another according to a lookup table.
- **Shift Rows:** a transposition step where each row of the state is shifted cyclically a certain number of steps.
- **Mix Columns:** a mixing operation which operates on the columns of the state, combining the four bytes in each column
- Add Round Key.

4. *Final Round (no Mix Columns):*

1) Sub Bytes.
2) Shift Rows.
3) Add Round Key.

3.2. Different Modes of AES

Block ciphers are encryption or decoding schemes in which a block of plaintext is treated as a single block and used to produce a block of code text of the same size [1]. AES (High level Encryption Standard) is currently one of the calculations for block encryption that requires the most complexity. It was standardized by the NIST (Public Foundation of Guidelines and Innovation) in 2001 to replace the DES and 3DES encryption algorithms that were in use at the time. The encryption key can be 128, 192, or 256 bits in size, but an AES block is only ever 128 bits in size. Four capabilities are used in each encryption phase: replacement of bytes, stage, number-crunching operations over constrained fields, and an XOR operation with the encryption key.

The AES block's size provides both competence and sufficient security. It has been hypothesized that the base size of the encryption key of 128 bits provides protection from animal power assaults given the figuring power of innovation at the time of the AES normalization and the expected processing power anticipated for the future [2]. Additionally, the calculation was built to be impervious to all hinder figure assaults which were known at that point. Block figure calculations ought to empower encryption of plaintext with size which is unique in relation to the characterized size of one block too. A method for giving this is introduced in [2, 3]. In particular, it is proposed to add a "1" to the plaintext which is more modest than the block, and add

"0's" cushioning to achieve the necessary size. Another way is to utilize a method of activity.

The calculation could be made more productively by using the block figure on a flood of plaintext in conjunction with the activity method. To strengthen the effect of the encryption calculation, however, the method of activity might convert the block figure into a stream figure. Five methods of activity—ECB (Electronic Code Book), CBC (Code Block Chaining), CFB (Code Feedback Mode), OFB (Output Feedback Mode), and CTR (Counter)—that apply to AES were normalized by the NIST in 2001 to satisfy these requirements [4].

Every method of activity has its own limitations, which are essential to providing the calculation with the fundamental security it needs. The five AES methods of operation will be described, along with any unique security boundaries. The first episode of the show will feature the ECB, CBC, CFB, OFB, and CTR standards of activity as they are described in the writing. The fundamental constraints, their advantages and disadvantages, as well as their legal application, will be discussed for each activity method. No matter what product or equipment is being used, the methods of activity are the most important for a legitimate AES execution. An ill-advised execution or utilization of the methods of activity may truly compromise the AES calculation unwavering quality and lead to divulgence of a section or all of the plaintext [5].

3.2.1. ECB Mode of Operation

The simplest mode of operation is ECB (Electronic Code Book). Blocks (P1, P2, PN) of the plaintext message are separated, and each block is encrypted separately using the same key (K). The encrypted messages C1, C2, and CN are the various outcomes of the encryption.

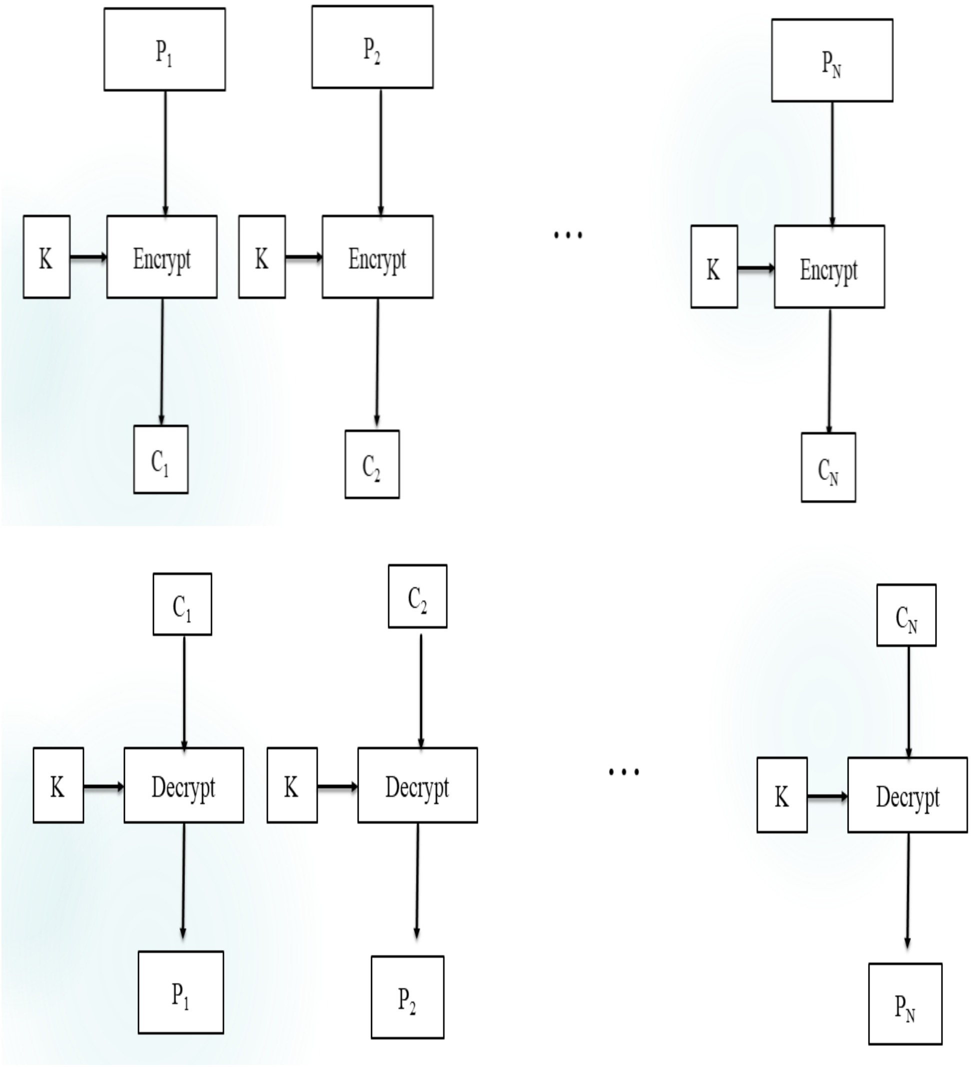


Figure 3.1: Scheme of the ECB mode of operation

In the event that the message size exceeds n obstructs, padding is loaded into the final block. Unscrambling is possible in the blocks without a mistake because, in this mode, if a mistake occurs in one of the blocks, it won't spread to the other blocks. According to [6], the encryption in this mode is deterministic because indistinguishable P blocks will result in indistinguishable C blocks, making a message with a similar start or indistinguishable plaintext blocks practically unmistakable. Additionally, it is possible to change the request for the C blocks without the recipient noticing. Generally speaking, this mode is not advised for the encryption of data that is larger than one block. According to [3], it is strictly forbidden to use this mode, and [7] declares that it is an outdated and abandoned activity.

3.2.2. CBC Mode of Operation

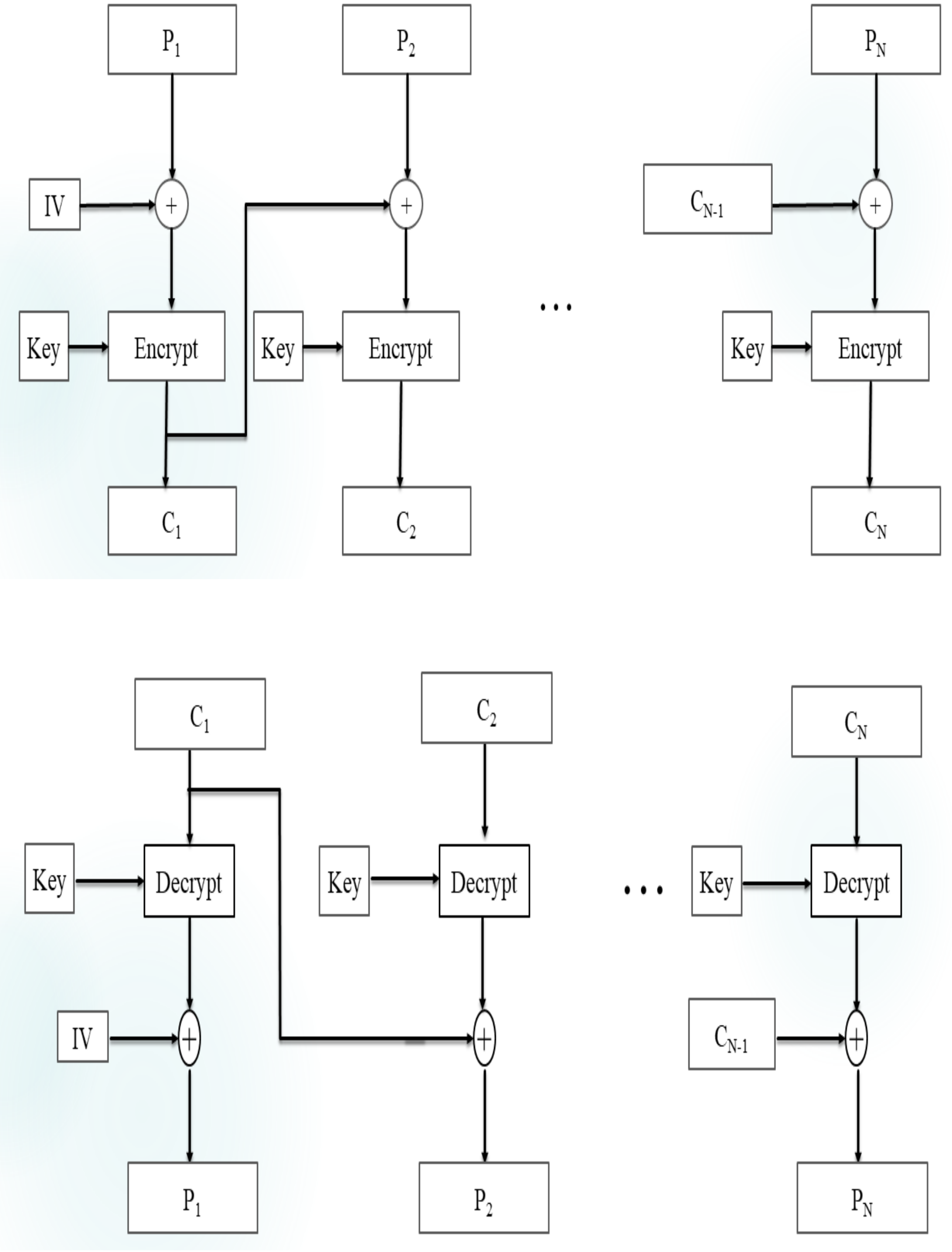


Figure 3.2: Scheme of the CBC mode of operation

Each encryption of the identical plaintext should produce a different code text in order to provide cryptographic security. This is provided by the CBC (Cipher Block Chaining) method of activity using an IV-based instatement vector. The IV is the exact same size as the encoded block. The plaintext block (P1) is first subjected to an XOR operation with the IV, and then the key (K) is used for encryption. The results of the encryption performed on each block (C1, C2,..., CN-1) are then used in an XOR operation on the subsequent plaintext block PN to produce CN. Along these lines, a different result is obtained when identical plaintext blocks are scrambled. A similar indistinguishable message will always be encoded in an unexpected manner by using a different IV for each new encryption. It should be noted that a single key, K, is used for all of the encryption blocks.

3.2.3. CFB Mode of Operation

The block encryptor may be used as a stream figure thanks to the CFB (Cipher Feedback Mode) method of operation. In the CFB method of operation, the encryption (which employs an encryptor indicated with Encode) is carried out by using an IV and an encryption key K at the beginning (at the primary block). The plaintext block (P1) and the encryption result (the result structure produced by the encryptor) are then subjected to an XOR operation. The encryption is carried out over the appropriately over the aftereffect of the encryption of the prior blocks for the vast array of different blocks (C1, C2, ...). The comparing plaintext block is then used in an XOR at that point (P2, P3, ...).

The IV is first placed in a shift register, which might have, for instance, 64 pieces in it. The IV's encryption has resulted in 64 pieces once more. However, a small number of pieces (say, s=8) of the encoded IV are subjected to an XOR operation with an equal number of bits from the plaintext P1. The least important IV components that won't be used are discarded. The XOR activity is then repeated in a manner similar to the first time, with the result C1from the XOR activity placed at the position in the shift register that is farthest to the right from the next block. In the CFB method of activity, the tasks of encrypting and decrypting are comparable [2, 6].

The IV is first placed in a shift register, which might have, for instance, 64 pieces in it. The IV's encryption has resulted in 64 pieces once more. However, a small number of pieces (say, s=8) of the encoded IV are subjected to an XOR operation with an equal number of bits from the plaintext P1. The least important IV components that won't be used are discarded. The XOR activity is then repeated in a manner similar to the first time, with the result C1from the XOR activity placed at the position in the shift register that is farthest to the right from the next block. In the CFB method of activity, the tasks of encrypting and decrypting are comparable [2, 6].

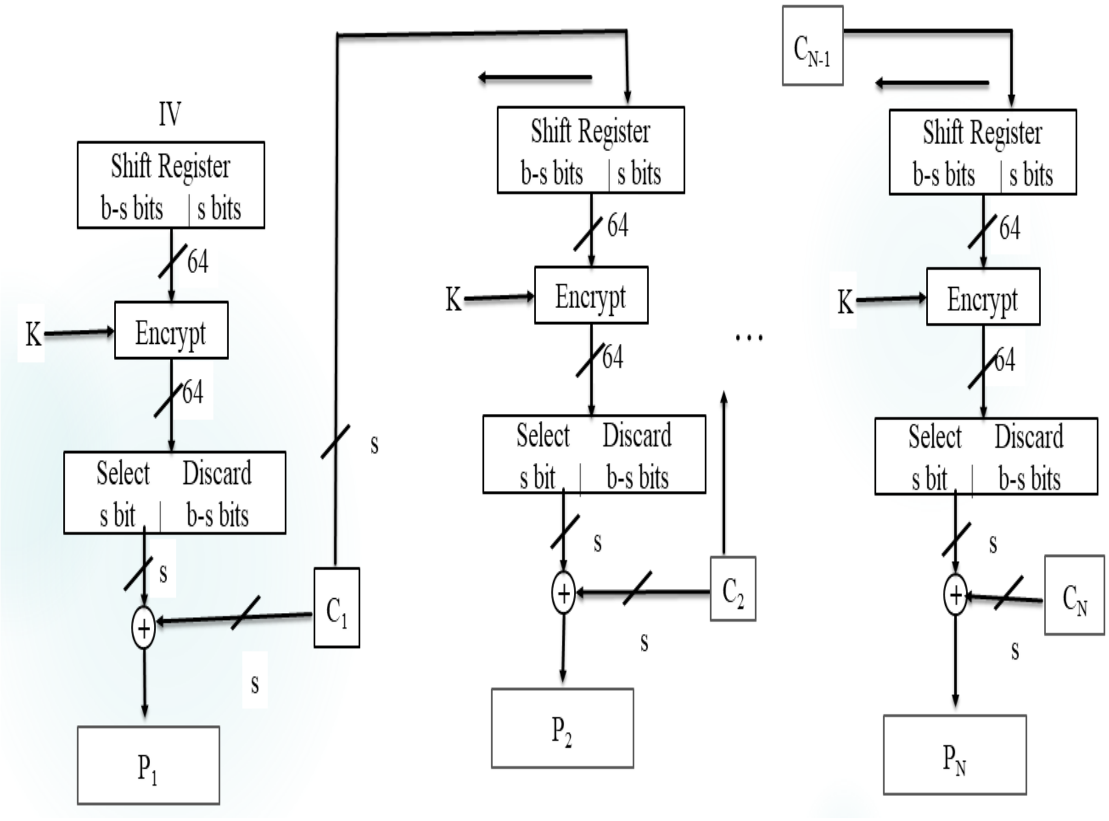
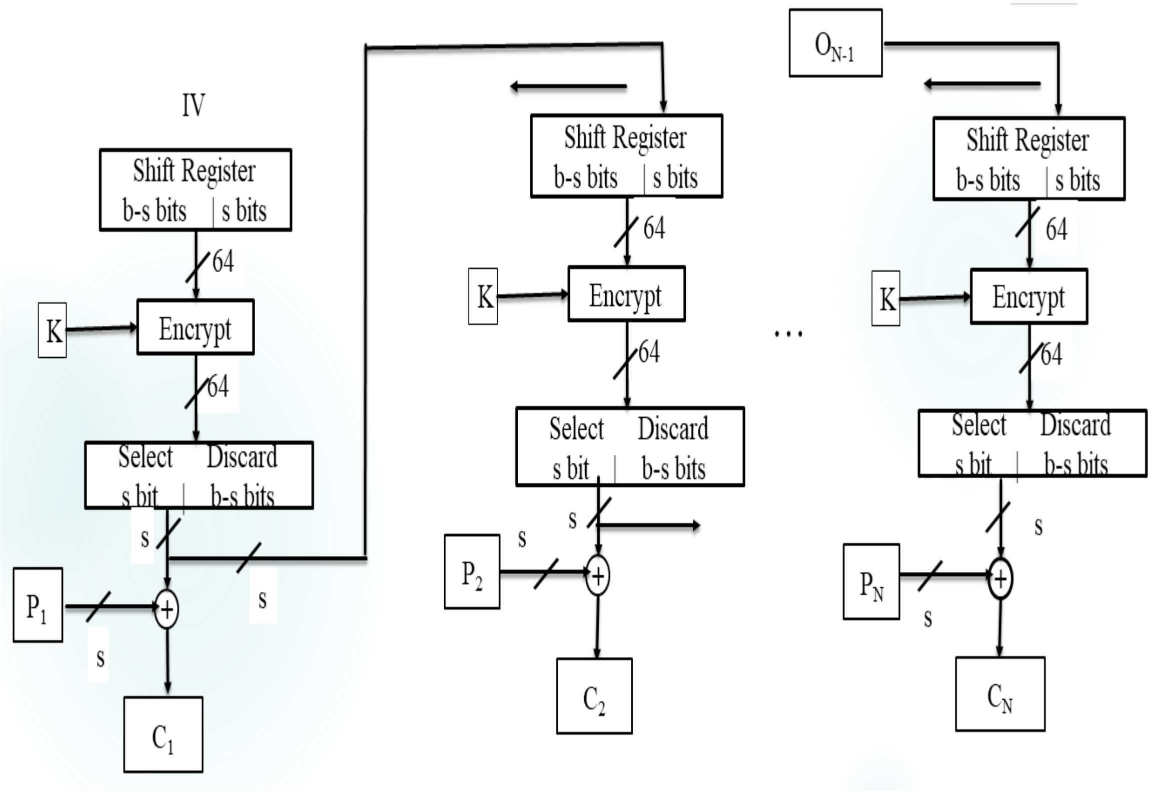


Figure 3.3: Scheme of the CFB mode of operation

3.2.4. OFB Mode of Operation

A block encryptor can also be used as a stream encryptor thanks to the OFB (Output FeedBack) mode of operation. The difference between the CFB and OFB modes is that, in the case of an OFB, the output from the encryptor (Encrypt) from the previous block is chosen as an input for the shift register from the next block. At the same time, only s bits from the encryptor are used in the XOR operation with the s-bits of plain text P. The operations of encryption and decryption are identical [6]. There is a limited propagation of error, meaning that if an error occurs in a block during encryption, it will only have an impact on a portion of the plain text that is generated from that block during decryption [2, 3]. As a result, this mode of operation is frequently used in communication via noisy media (for example, satellite communications).

The IV should be a nonce, claims [6]. According to the instructions in [8], the IV should be selected at random and should only be used once with the provided encryption key K. Security cannot exist if the IV is a nonce, according to [7], but the sequence produced by some counter is acceptable. Attacks that alter bits in the encrypted stream can be made against the CFB mode of operation [2]. The encryption key K should be changed every 2n/2 encryption blocks, where n is the number of bits in a block, to ensure security in the OFB mode of operation [3]. However, [7] makes clear that the OFB does not provide protection from CCA attacks.



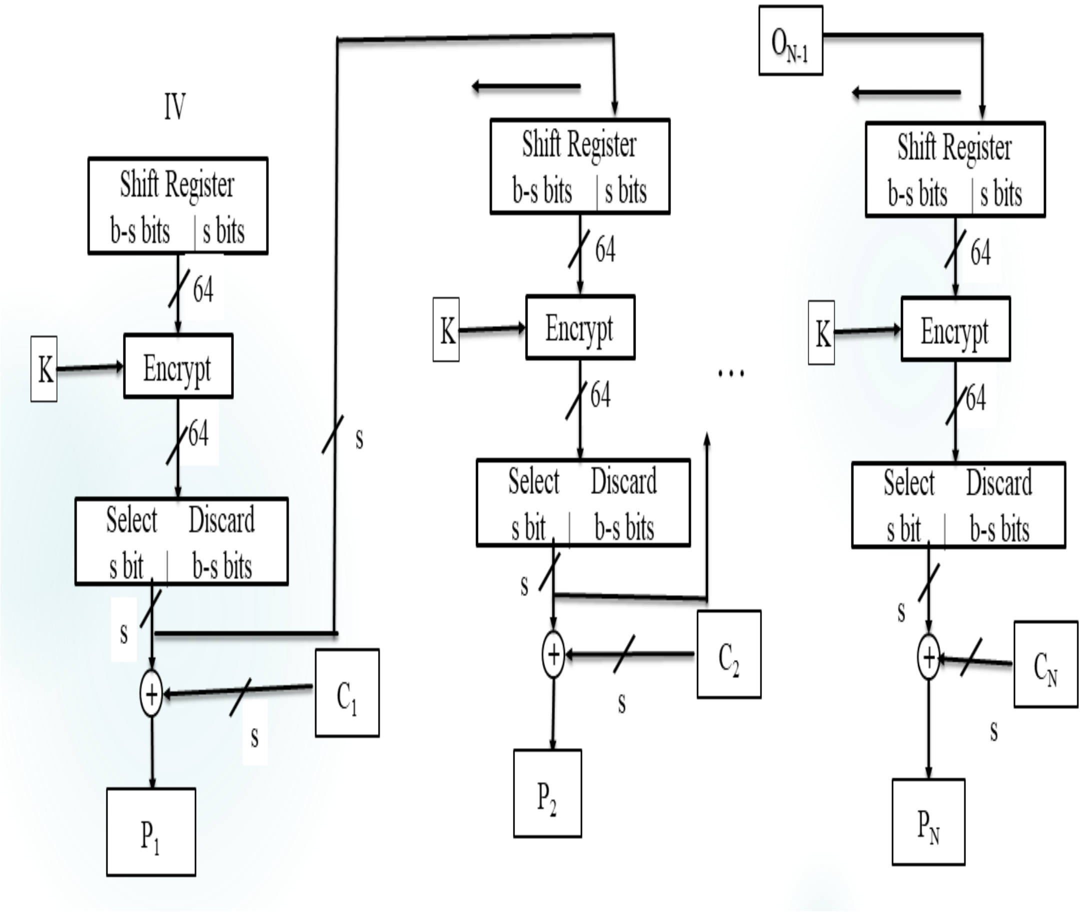


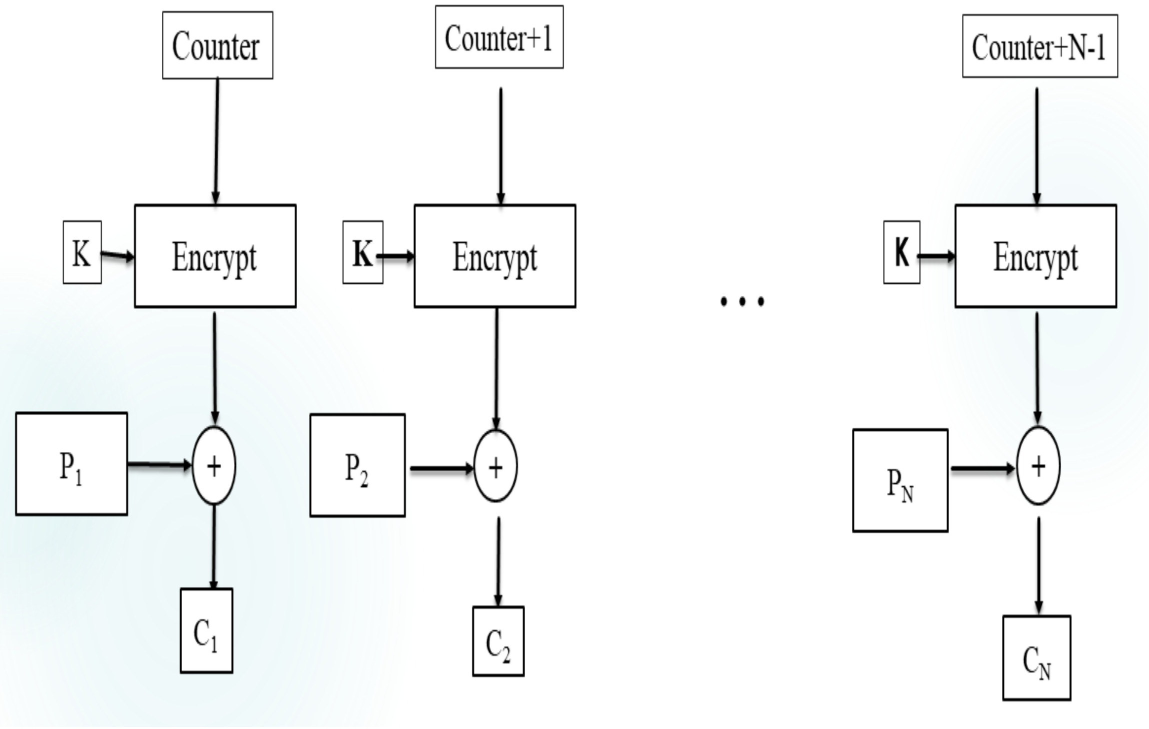
Figure 3.4: Scheme of OFB mode of operation

3.2.5. CTR Mode of Operation

When using the CTR (Counter) method of operation, an information block to the encryptor (Encode), such as an IV, is valued using a counter (Counter, Counter + 1,..., Counter + N - 1). The counter and the used block are of comparable size [2]. The result block from the encryptor is then subjected to an XOR operation with the block of plain text (P1, P2,..., PN). The same encryption key K is used by all encryption blocks. Only the largest pieces from the result block of the encryptor are used for the XOR operation on the block PN if the last block of clear text PN has a smaller number of pieces than the number of pieces in the block. The extra pieces are thrown away. Therefore, as is pointed out in [4], there is no need to add pieces (cushioning) to the final block. The counters' upsides aren't affected by the outcomes of previous blocks, so mistakes don't accumulate from one block to the next [5, 8].

This reality takes the freedom of the blocks into account and parallelizes the encoding and decoding processes. There is also the possibility of preprocessing the advantages of the encryptors [2], which shortens the cycle. At the CTR method of activity, the tasks of encrypting and decrypting are equivalent [8]. Each block should have a different counter grouping [4]. However, it is suggested in [5] and [6] that a similar counter value (Counter, Counter + 1, Counter + N - 1) and a similar key K shouldn't be used in that context of more than one block of information. If this condition is not met, it is possible to decode the plaintext by performing an XOR operation on two blocks of text that have similar boundary arrangements. All things considered, a security breach has occurred [7].

The counter is typically introduced to a certain value and then increased by one for each block [2]. It is explained in [6] that the counter's introducing worth is a non-repeatable number on the order of 96 pieces. At the beginning of the process, the qualities of the remaining 32 pieces are zero. Later, for each block, their qualities increase by 1. The guidelines in [8] recommend giving the Counter a special incentive that is chosen erratically. The encryption key K needs to be changed every 2n/2 blocks of encryption, where n is the number of pieces in a block, in order to ensure security with the CTR [3]. The CTR mode is distinguished as the most ideal option among all the others based on the methods of activity in [7]..



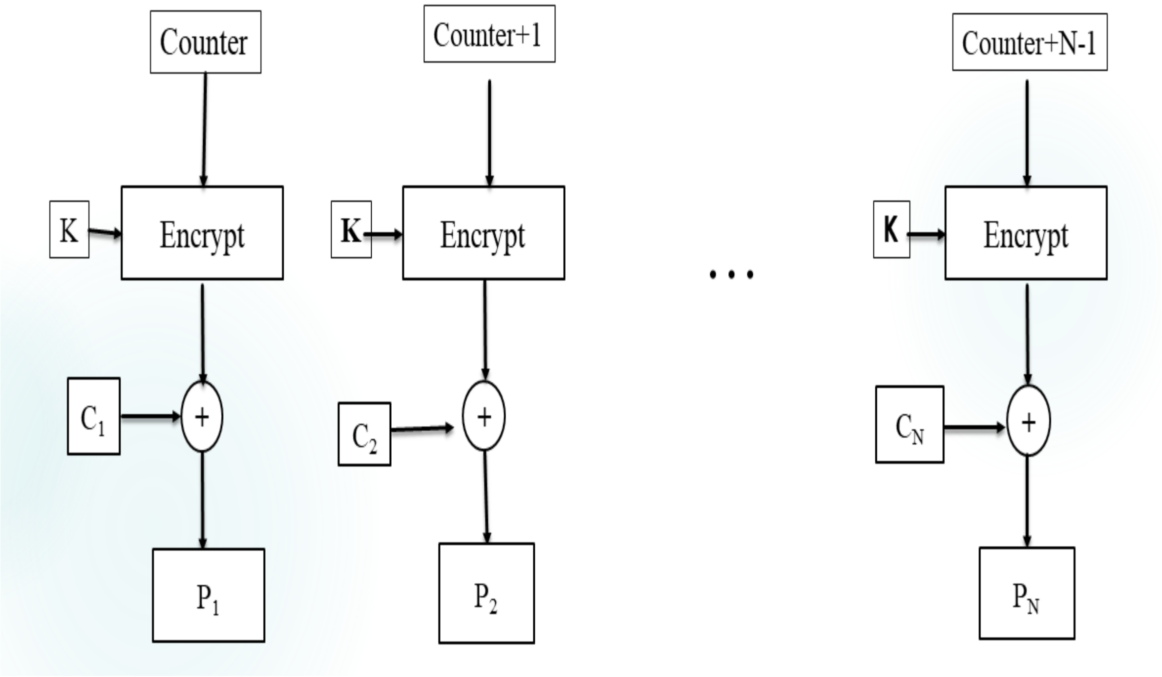
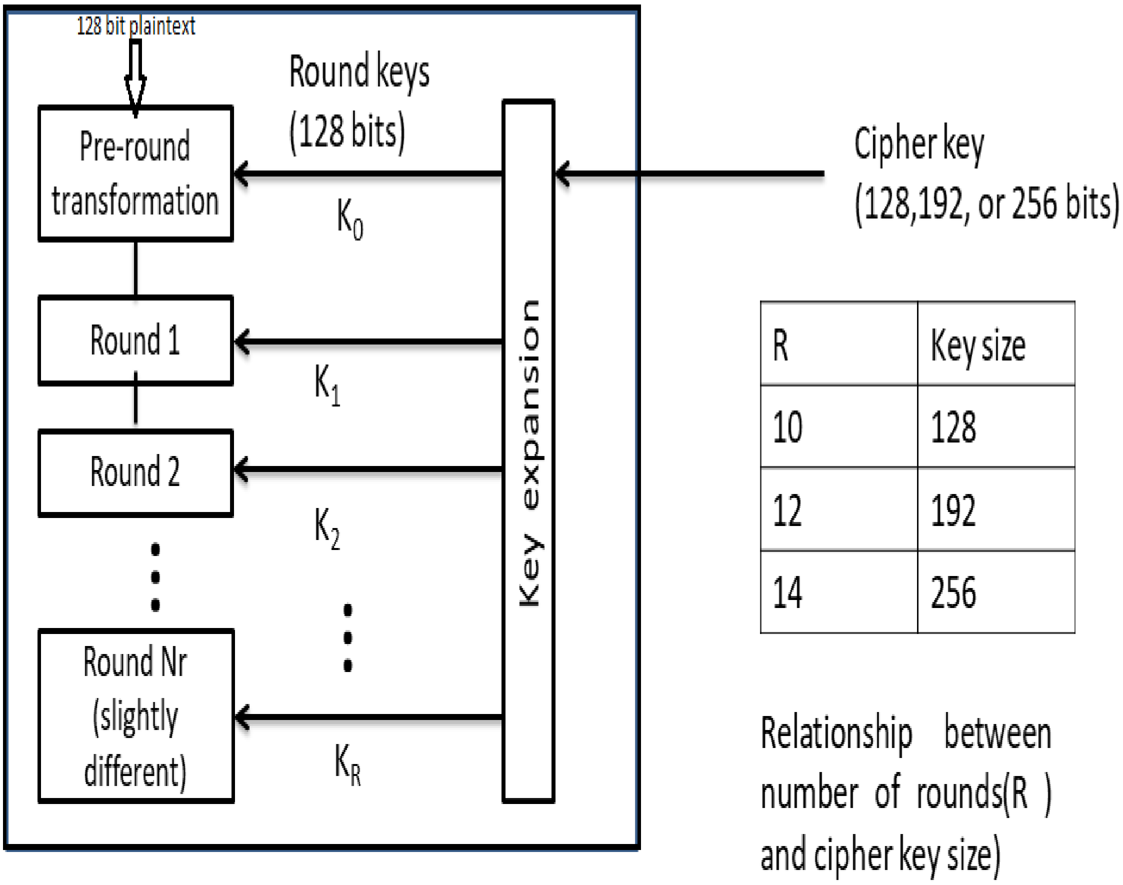


Figure 3.5: Scheme of CTR mode of operation

CHAPTER 4

DESIGN AND IMPLEMENTATION OF SYSTEM

The Advanced Encryption Standard (AES) algorithm is a symmetric key encryption algorithm. AES uses keys with lengths of 128 bits, 192 bits, and 256 bits. Every block of 128 bits is divided by the AES algorithm into 16 bytes. Each 16-byte segment is resolved as a 4-by-4 matrix. The number of rounds depends on the size of the key. The plaintext must be divided into multiple blocks if its length exceeds the block size. Normally, the plaintext's final block needs to be padded to fit the block size.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size)

Figure 4.1: AES algorithm grouping and encryption diagram

The majority of network-based symmetric cryptographic applications employ AES. Substitutions (also known as S-Box) and permutations are used in a series of mathematical operations called the substitution-permutation process, or AES (P-Boxes).

Steps of AES algorithm:

1) Key Expansion
2) Initial round
    a. Add-Round-Key
3) Nr -1 Round
    a. Sub-Bytes
    b. Shift-Rows
    c. Mix-Columns
    d. Add-Round-Key
4) Final Round
    a. Sub-Bytes
    b. Shift-Rows

AES uses variable number of rounds (Nr) which are fixed: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. During each round, above operations are applied on the state as shown in figure 1.

- **Sub-Bytes:** The substitute bytes operation is a nonlinear byte substitution that modifies the byte values while operating independently on each of the state bytes using an S-box.
- **Shift-Row:** Depending on the row index, each row in the 4x4 array is moved to the left by a specific amount.
- **Mix-Column:** The mix columns transformation acts on four values at once as though they represented a four-term polynomial in order to transform the values of a given column within a state.
- **Add-Round-Key:** Round keys are used to combine each byte of the state; each key is unique.

4.1 Cipher block chaining (CBC) Mode

Through the use of an introduction vector-IV, the CBC method of operation provides cryptographic security. IV is the exact same size as the confused block. The IV is typically an erratic number, on average. When identical plaintext blocks are encoded in CBC mode, an alternative code text block is obtained. Similar to using a different IV for every new encryption, an identical message will always be encoded unexpectedly. A broken plaintext or figure text block will have an impact on all blocks that follow. Numerous applications, including email and web information, use the CBC mode. In the diagram, the plaintext block (P1) is first subjected to an XOR operation with the help of the IV, and then the key (K) is used to encrypt the data. The results of the encryption performed on each block (C_1, C_2,..., C_{N-1}) are then used in an XOR operation on the subsequent plaintext block PN to produce C_N.

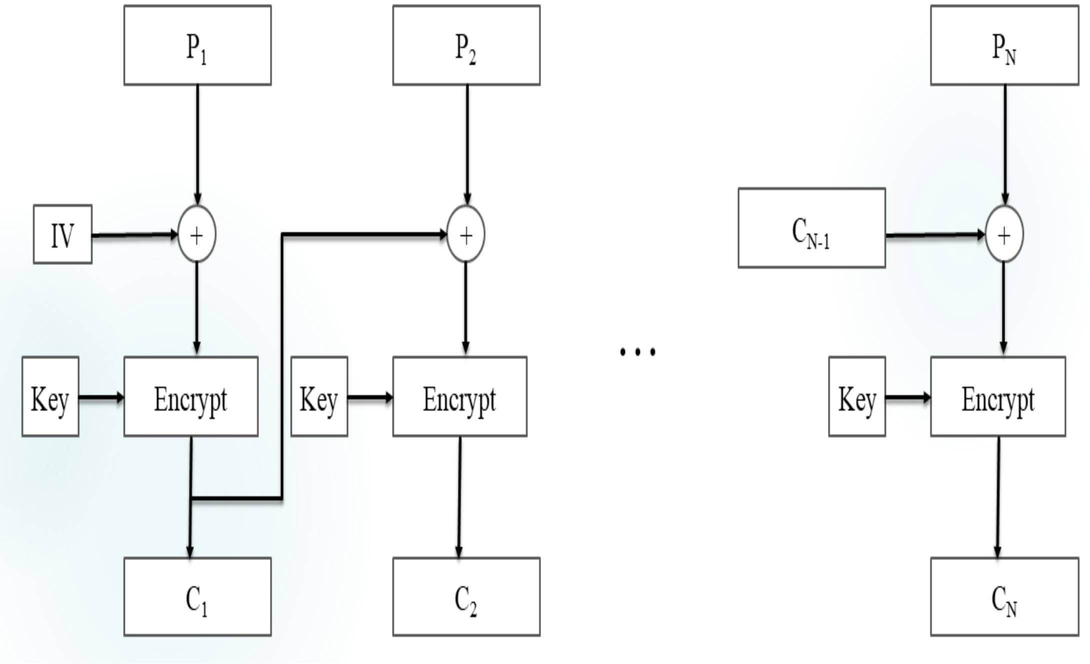


Figure 4.2.1: Encryption in the CBC Mode

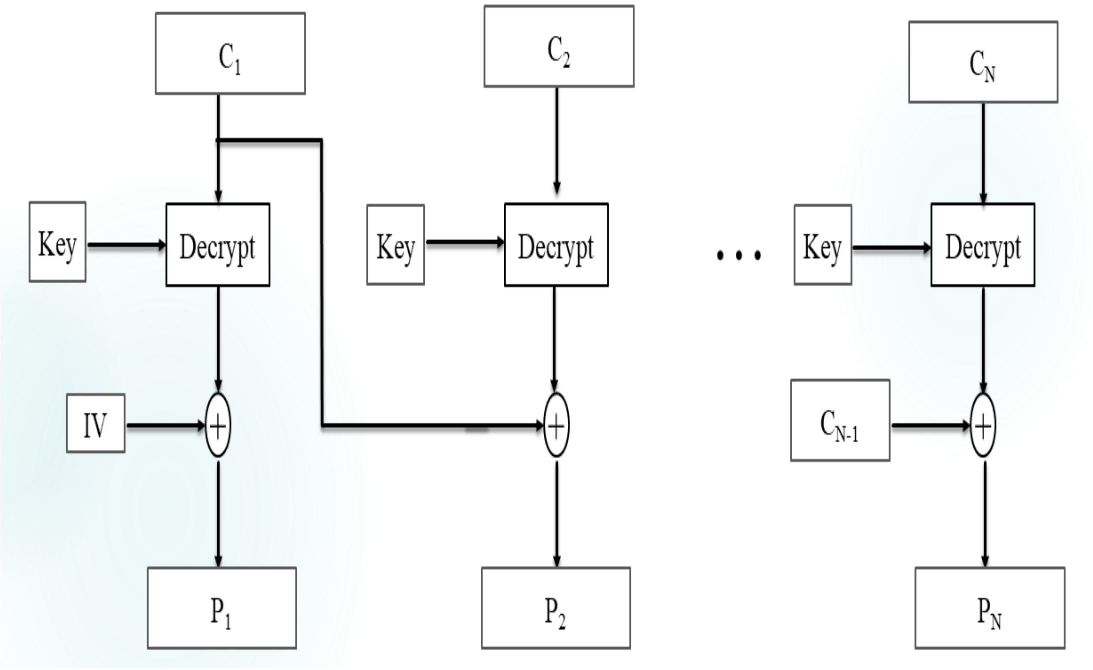


Figure 4.2.2: Decryption in the CBC Mode

4.2 Initialization Vector (IV)

An initialization vector (IV) or starting variable (SV) is a component of a cryptographic crude that is used to provide the underlying state in cryptography. The IV is typically anticipated to be arbitrary or pseudorandom, but occasionally an IV just needs to be erratic or exceptional. Some encryption schemes require randomization in order to achieve semantic security. The pseudorandom (Linear Congruential Generator) will be used in this framework as IV.

Linear Congruential Generator

- A polynomial-time computable function f (x) that expands a short random string x into a long string f (x) that appears random.
- Based on the linear recurrence:
- $x_i = ax_{i-1} + b \bmod m$ ………. ($i \geq 1$)
- Where x_0 is the seed or start value; a is the multiplier; b is the increment; m is the modulus.

➢ Output → pseudo-random sequence of bits

4.3. Secure Key Sharing

Secure file transfer protocols like FTPS, HTTPS, and SFTP must encrypt the data using symmetric encryption in order to maintain data confidentiality during transmission. In order for the two communicating parties to encrypt and decrypt messages using this type of encryption, they must have a shared key. However, it is difficult to allow two parties to use a shared key, which is the issue. The key cannot simply be sent via conventional channels because anyone who obtains it will be able to decrypt all the files that the two parties will be exchanging. ELGamal will therefore be in charge of managing this proposed system's secure key sharing.

EL-Gamal Cryptosystem

An asymmetric key encryption algorithm for public key cryptosystems is the ELGamal system.

▶ Key aspects:

•Randomized encryption

▶ Application:

•Establishing a secure channel for key sharing

•Encrypting messages

Taher ELGamal provided a description of the ELGamal encryption algorithm. The open-source GNU Privacy Guard program, more recent iterations of PGP, and other cryptosystems all employ ELGamal encryption. The key generator, the encryption algorithm, and the decryption algorithm are the three parts of the ELGamal encryption system.

ELGamal Cryptosystem – Key Generation

```
{
        Select a large prime p;
        Select d to be a member of the group $G = < Z_P^*, X >$ where $1<= d<= p-2$
        Select $e_1$ to be a primitive root in the group $G = < Z_P^*, X >$
        $e_2 \leftarrow e_1^{d} \bmod p$
        Public_key ← $(e_1, e_2, p)$
        Private_key ← d
        return Public_key and Private_key
}
```

ELGamal Cryptosystem-Encryption Procedure

```
ElGamal_Encryption (e1,e2, p, P)      // P is the plaintext
{       Select a random integer r in the group $G = < Z_P^*, X >$
        $C_1$ ← $e_1^r$  mod  p
        $C_2$ ← ( P x $e_2^r$ ) mod p        // $C_1$ and $C_2$ are ciphertexts
        return $C_1$ and $C_2$  }
```

ELGamal Cryptosystem-Decryption Procedure

```
ElGamal_Decryption ( d, p, $C_1$, $C_2$ )
{
        P ← $[C_2 (C_1^d)^{-1}]$ mod p
        return P
}
```

4.4. Implementation of System

In this system: Data is authenticated between the sender and receiver before being sent. After successful authentication, the user can send data to the recipient after it has been encrypted. The sender can create or choose the attach .doc / .xlsx file to send to the receiver. In the encryption and decryption phase, this system will used AES-CBC mode. In the proposed system, 256 bit key size of AES algorithm is used to do the evaluation of the operation mode of CBC. The AES-CBC key is encrypted by Elgamal for secure key sharing.

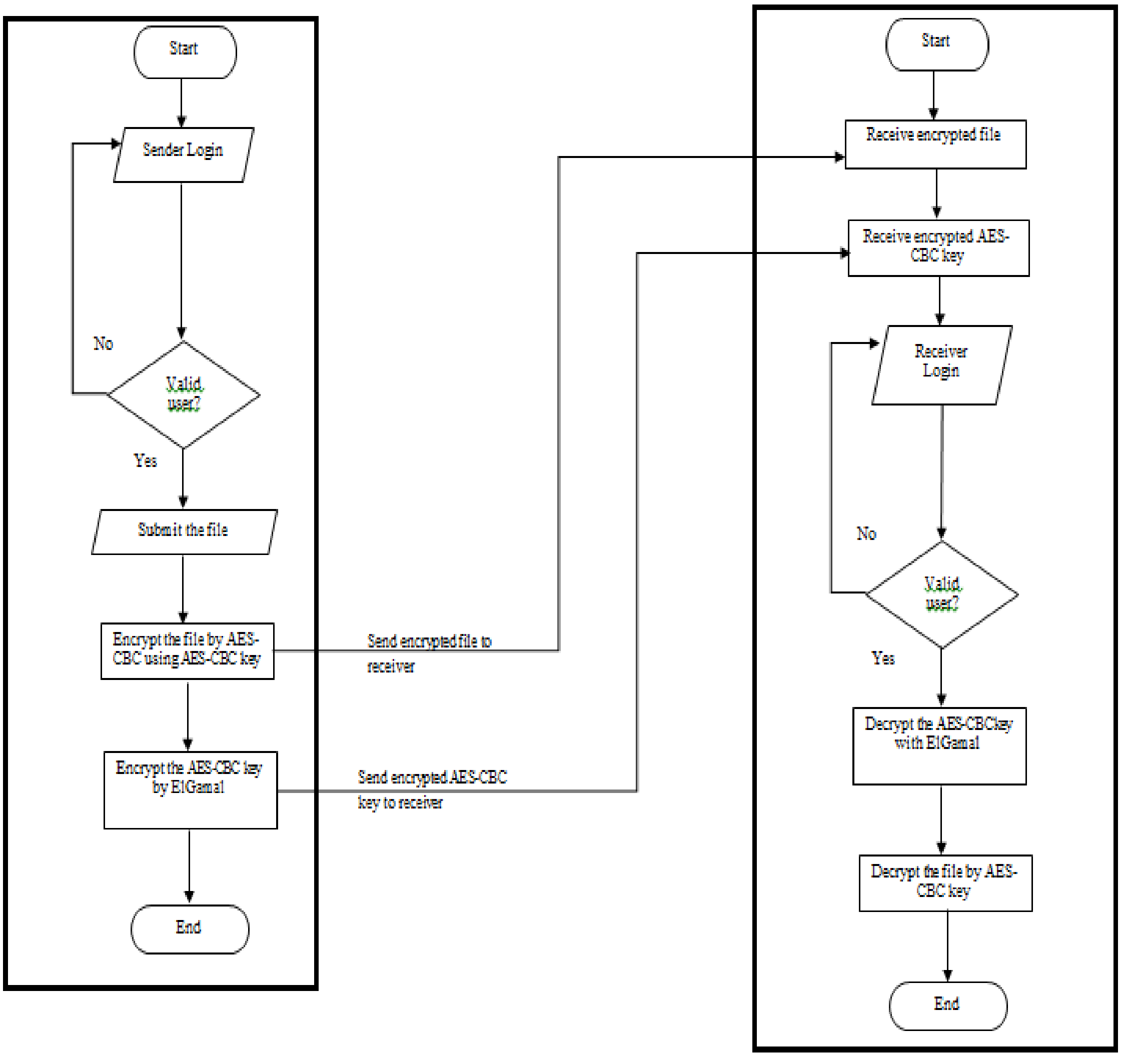
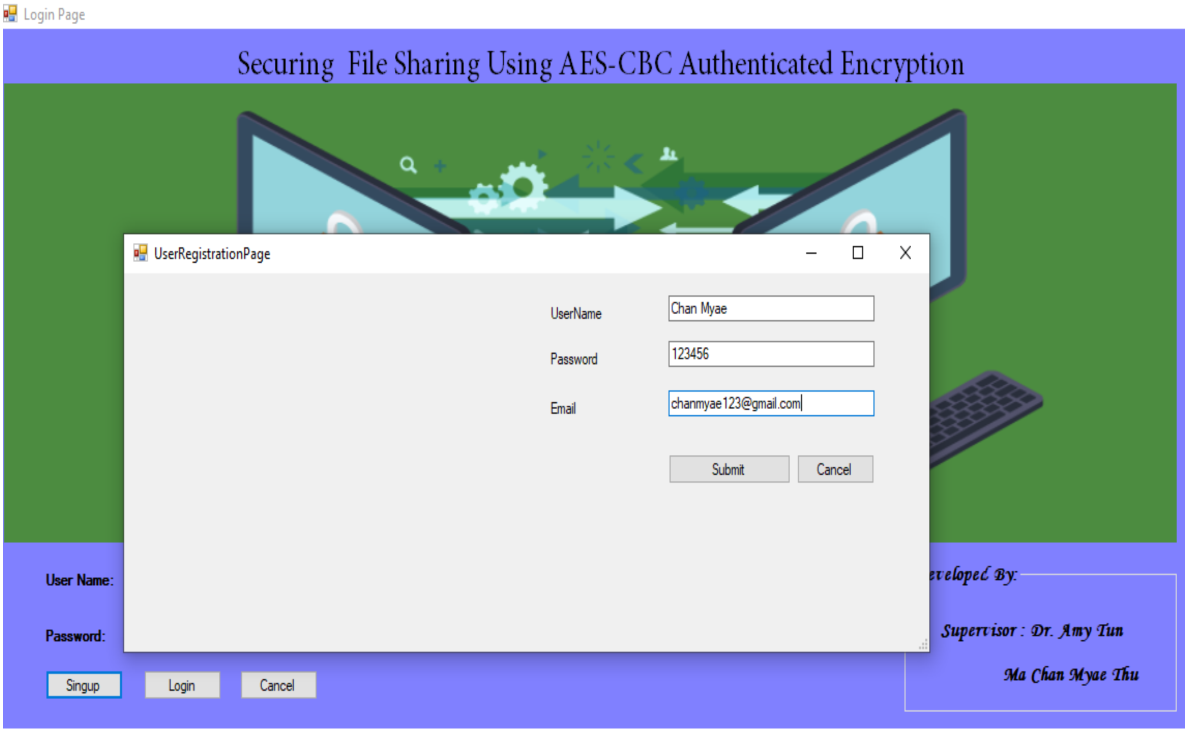

Start
Sender Login
No
Valid user?
Yes
Submit the file
Encrypt the file by AES-CBC using AES-CBC key
Encrypt the AES-CBC key by ElGamal
End
Send encrypted file to receiver
Send encrypted AES-CBC key to receiver
Start
Receive encrypted file
Receive encrypted AES-CBC key
Receiver Login
No
Valid user?
Yes
Decrypt the AES-CBCkey with ElGamal
Decrypt the file by AES-CBC key
End

Figure 4.3: The System Flow

Providing security for both online and offline email usage is of utmost importance because of the potential misuse of the data contained in private file sharing (whether working online or offline). In daily life, messaging is a crucial form of communication. Email is used for a variety of transactions, the transmission of crucial information, and simple correspondence. protecting the private messaging's data in the process.



Login Page

Securing File Sharing Using AES-CBC Authenticated Encryption

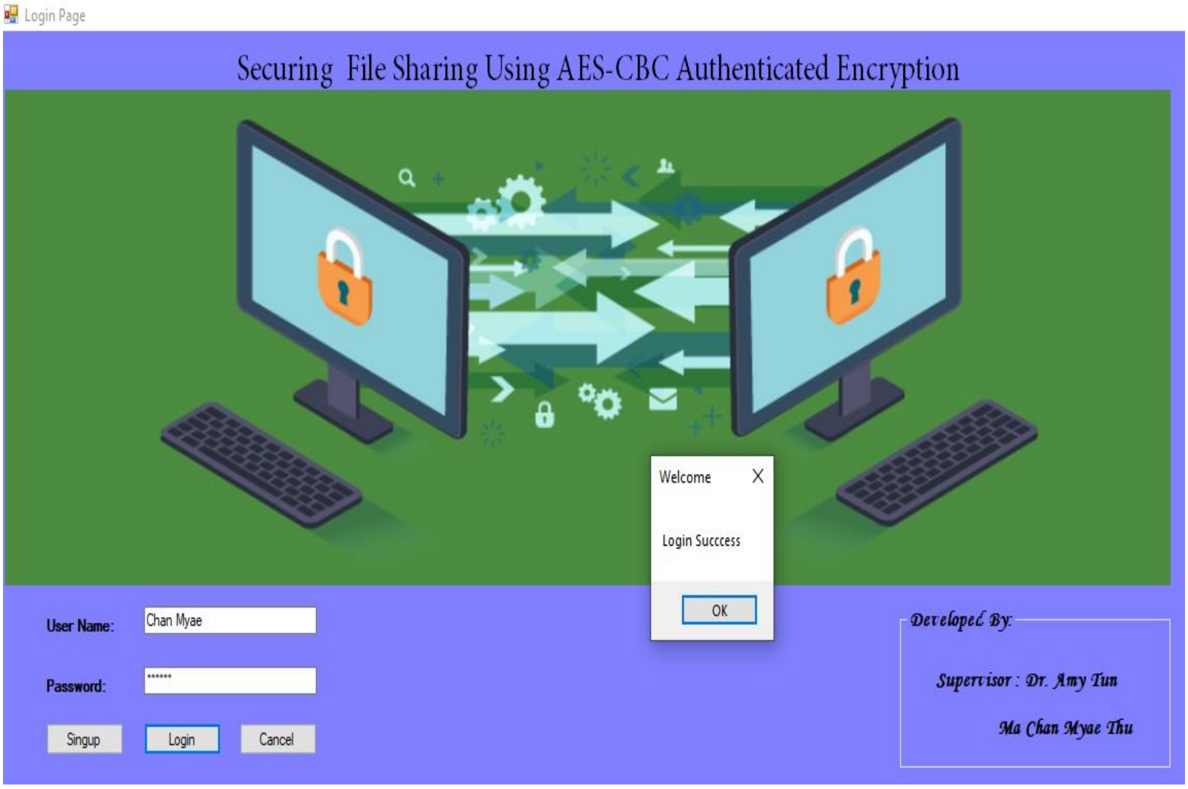
UserRegistrationPage

UserName: Chan Myae

Password: 123456

Email: chanmyae123@gmail.com

Figure 4.4: User Register Login



Login Page

Securing File Sharing Using AES-CBC Authenticated Encryption

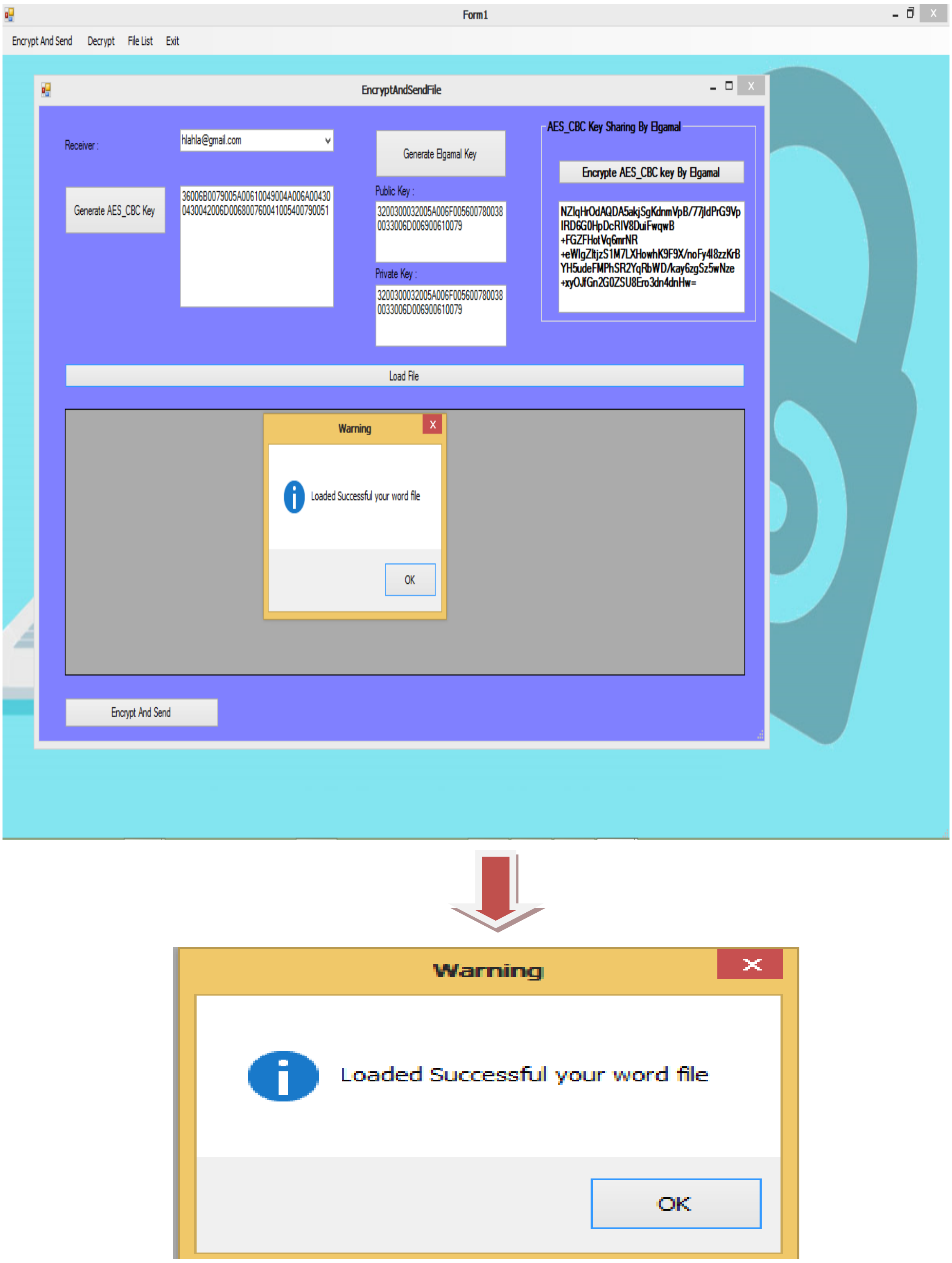
Welcome

Login Succcess

User Name: Chan Myae

Password: ******

Figure 4.5: User Login



Receiver : hlahla@gmail.com

36006B0079005A00610049004A006A00430
043004200 6D006800760041005400790051

Public Key :
3200300032005A006F005600780038
0033006D006900610079

Private Key :
3200300032005A006F005600780038
0033006D006900610079

NZIqHrOdAQDA5akjSgKdnmVpB/77jldPrG9Vp
IRD6G0HpDcRIV8DuiFwqwB
+FGZFHotVq6mrNR
+eWIgZltjzS1M7LXHowhK9F9X/noFy4l8zzKrB
YH5udeFMPhSR2YqRbWD/kay6zgSz5wNze
+xyOJfGn2G0ZSU8Ero3dn4dnHw=

Warning

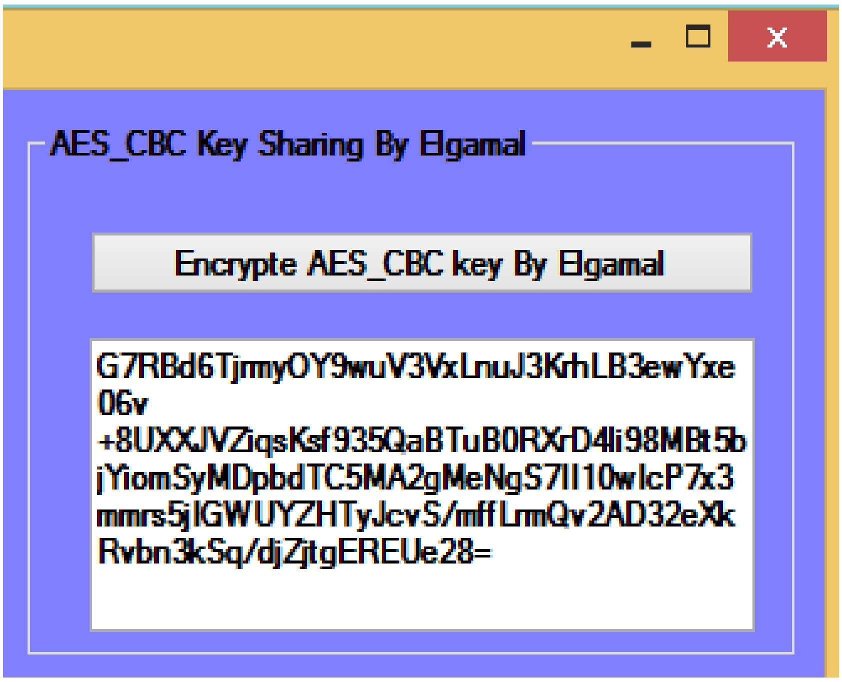
Loaded Successful your word file

Warning

Loaded Successful your word file

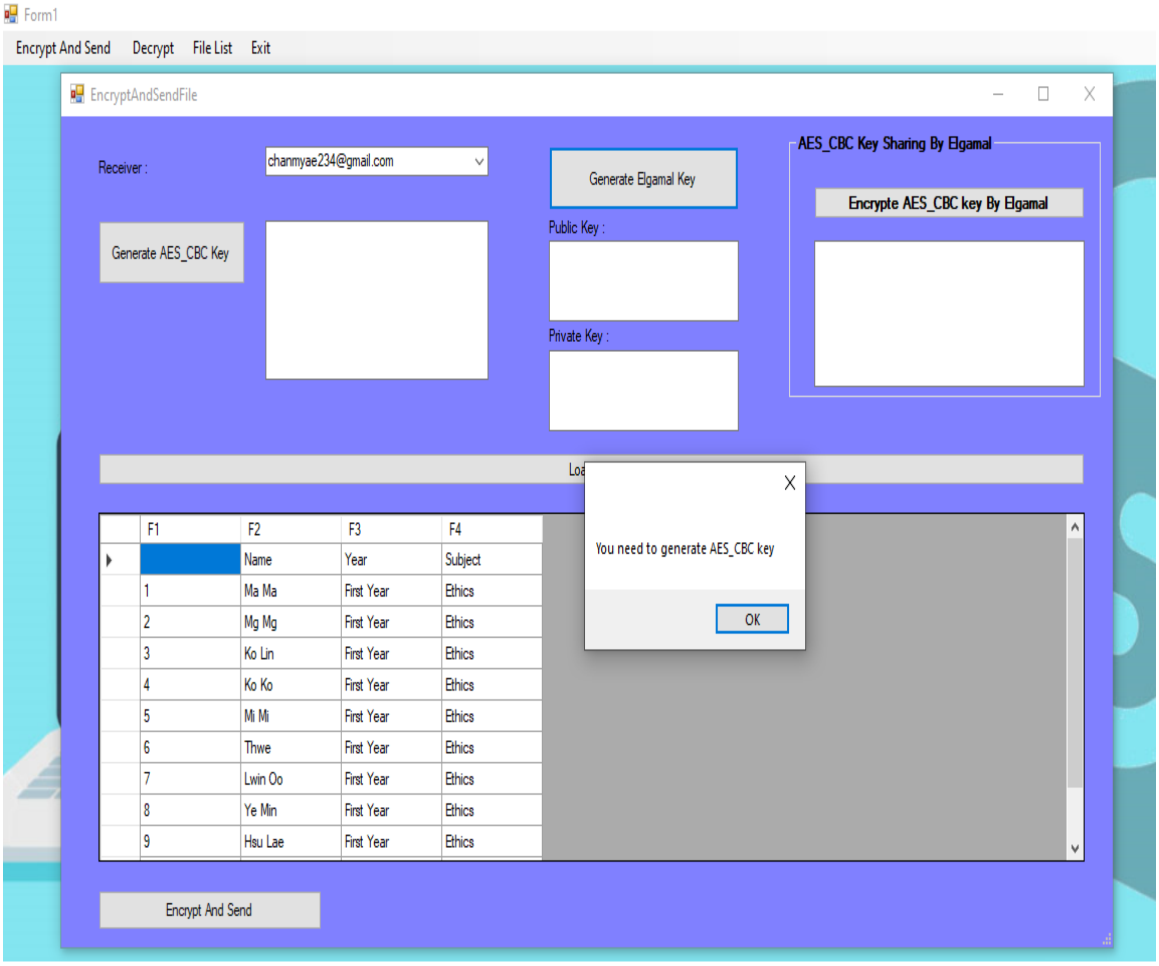
Figure 4.6: Message Encryption By AES-CBC (For Document File)

In this system: Authentication is carried out between the sender and the receiver prior to message sending or reading. Following successful authentication, the user can encrypt data before sending it to the recipient, as shown in figure 4.3. Then, the sending message encryption for the document file of the proposed system is as shown in figure 4.6 and the AES-CBC's key is encrypted by ELGamal for secure key sharing is show in figure 4.7.


AES_CBC Key Sharing By Elgamal
Encrypte AES_CBC key By Elgamal

```
G7RBd6TjmmyOY9wuV3VxLnuJ3KrhLB3ewYxe
06v
+8UXXJVZiqsKsf935QaBTuB0RXrD4li98MBt5b
jYiomSyMDpbdTC5MA2gMeNgS7lI10wlcP7x3
mmrs5jlGWUYZHTyJcvS/mffLmQv2AD32eXk
Rvbn3kSq/djZjtgEREUe28=
```

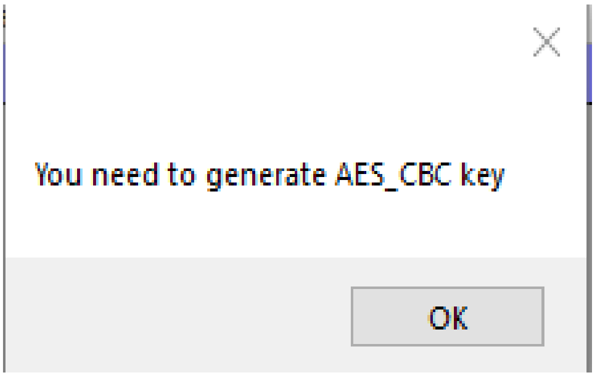
Figure 4.7: AES-CBC Key Encryption by ELGamal



Receiver : chanmyae234@gmail.com

F1	F2	F3	F4
	Name	Year	Subject
1	Ma Ma	First Year	Ethics
2	Mg Mg	First Year	Ethics
3	Ko Lin	First Year	Ethics
4	Ko Ko	First Year	Ethics
5	Mi Mi	First Year	Ethics
6	Thwe	First Year	Ethics
7	Lwin Oo	First Year	Ethics
8	Ye Min	First Year	Ethics
9	Hsu Lae	First Year	Ethics

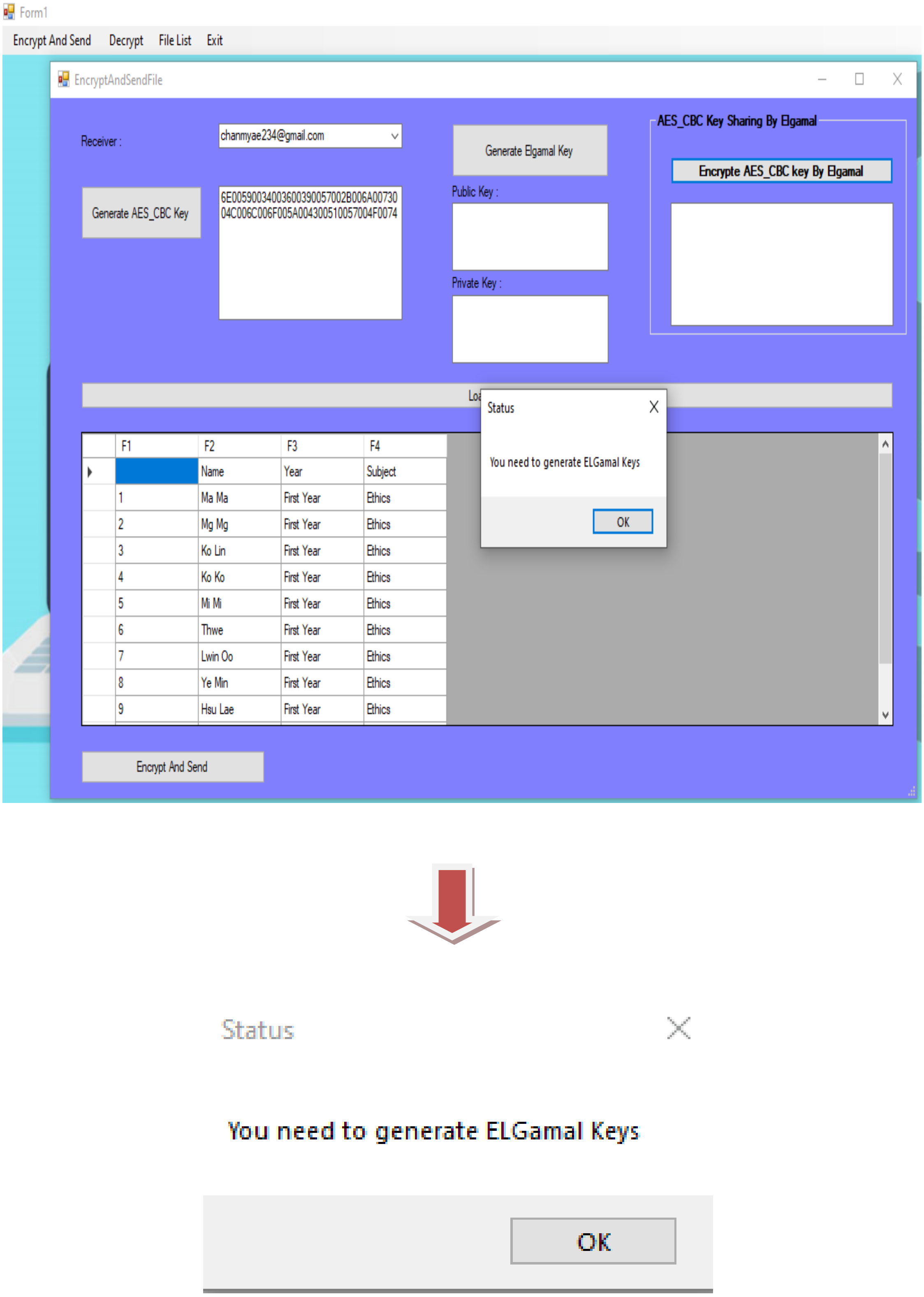
You need to generate AES_CBC key



You need to generate AES_CBC key

Figure 4.8: Message Encryption Need By AES-CBC Key

To scramble the succeed record, the AES-CBC's key is expected to encode on the off chance that the source is neglect to create AES-CBC Key for secure key sharing . The messsge box will give the data need to produce AES-CBC key is displayed in figure 4.8.



Receiver : chanmyae234@gmail.com

6E005900340036003900570028006A00730
04C006C006F005A004300510057004F0074

Public Key :

Private Key :

	F1	F2	F3	F4
▸		Name	Year	Subject
	1	Ma Ma	First Year	Ethics
	2	Mg Mg	First Year	Ethics
	3	Ko Lin	First Year	Ethics
	4	Ko Ko	First Year	Ethics
	5	Mi Mi	First Year	Ethics
	6	Thwe	First Year	Ethics
	7	Lwin Oo	First Year	Ethics
	8	Ye Min	First Year	Ethics
	9	Hsu Lae	First Year	Ethics

Status

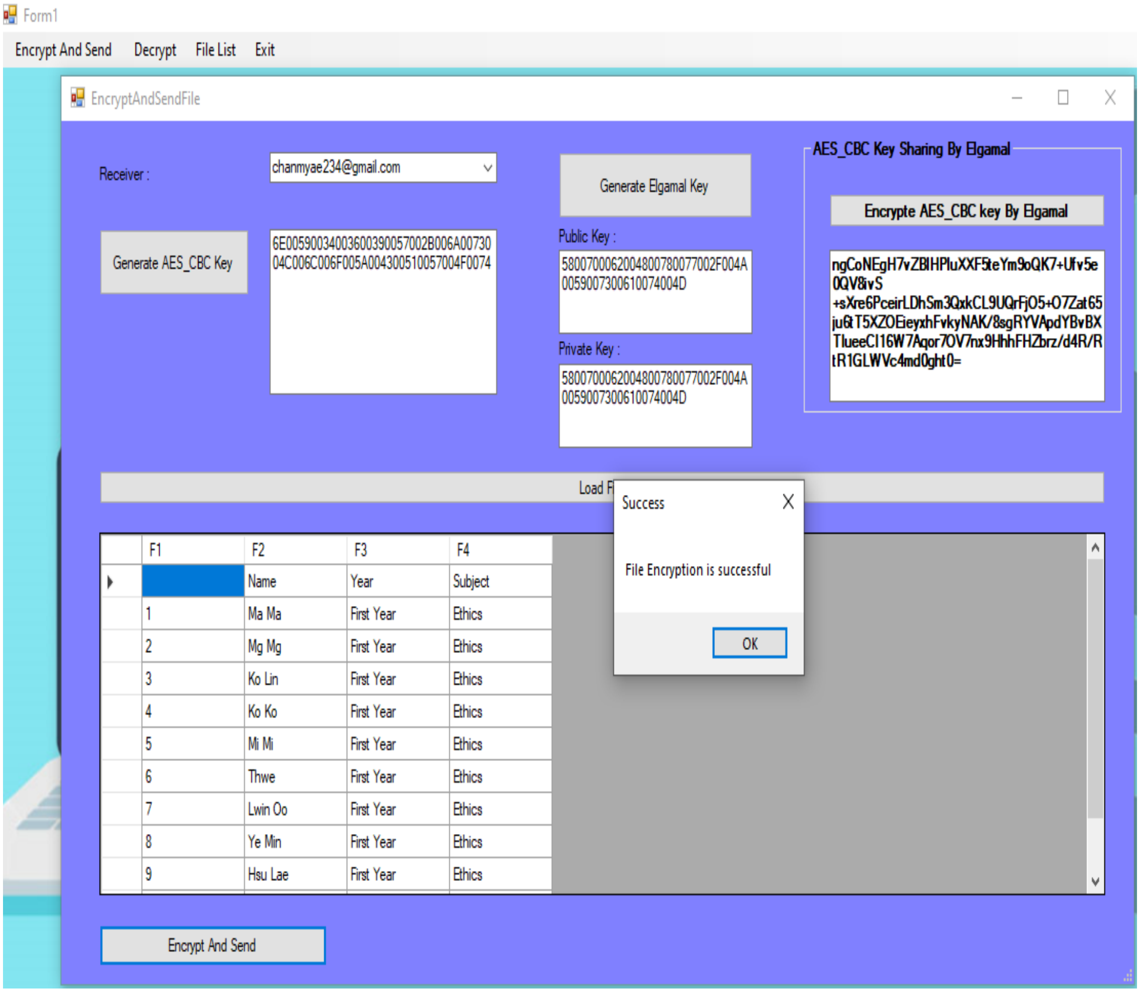
You need to generate ELGamal Keys

Status

You need to generate ELGamal Keys

Figure 4.9: Message Encryption Need By ElGamal Key

Assuming the source is tapped the encode AES-CBC key by Elgamal button without click the Create Elgamal Key button , the message box will give the data need to produce Elgamal Key which displayed in Figure 4.9.



Receiver : chanmyae234@gmail.com

6E00590034003600390057002B006A00730
04C006C006F005A004300510057004F0074

Public Key :
5800700062004800780077002F004A
0059007300610074004D

Private Key :
5800700062004800780077002F004A
0059007300610074004D

ngCoNEgH7vZBIHPluXXF5teYm9oQK7+Ufv5e
0QV8ivS
+sXre6PceirLDhSm3QxkCL9UQrFjO5+O7Zat65
ju6tT5XZOEieyxhFvkyNAK/8sgRYVApdYBvBX
TlueeCI16W7Aqor7OV7nx9HhhFHZbrz/d4R/R
tR1GLWVc4md0ght0=

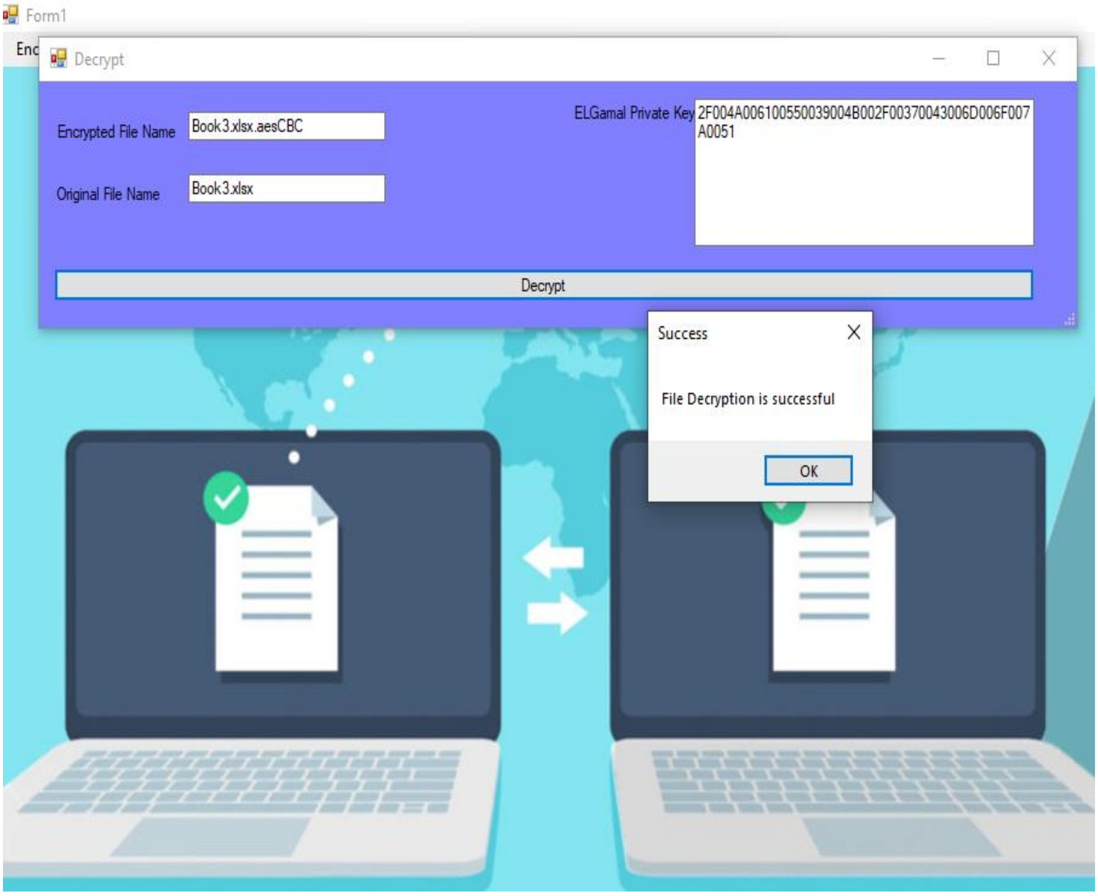
F1	F2	F3	F4
	Name	Year	Subject
1	Ma Ma	First Year	Ethics
2	Mg Mg	First Year	Ethics
3	Ko Lin	First Year	Ethics
4	Ko Ko	First Year	Ethics
5	Mi Mi	First Year	Ethics
6	Thwe	First Year	Ethics
7	Lwin Oo	First Year	Ethics
8	Ye Min	First Year	Ethics
9	Hsu Lae	First Year	Ethics

Success

File Encryption is successful

Figure 4.10: Successful Message Encryption

The getting message decoding for the succeed document of the proposed framework is as displayed in figure 4.10 and the AES-CBC's key is unscrambled by ELGamal private key for secure key sharing.



Encrypted File Name Book3.xlsx.aesCBC

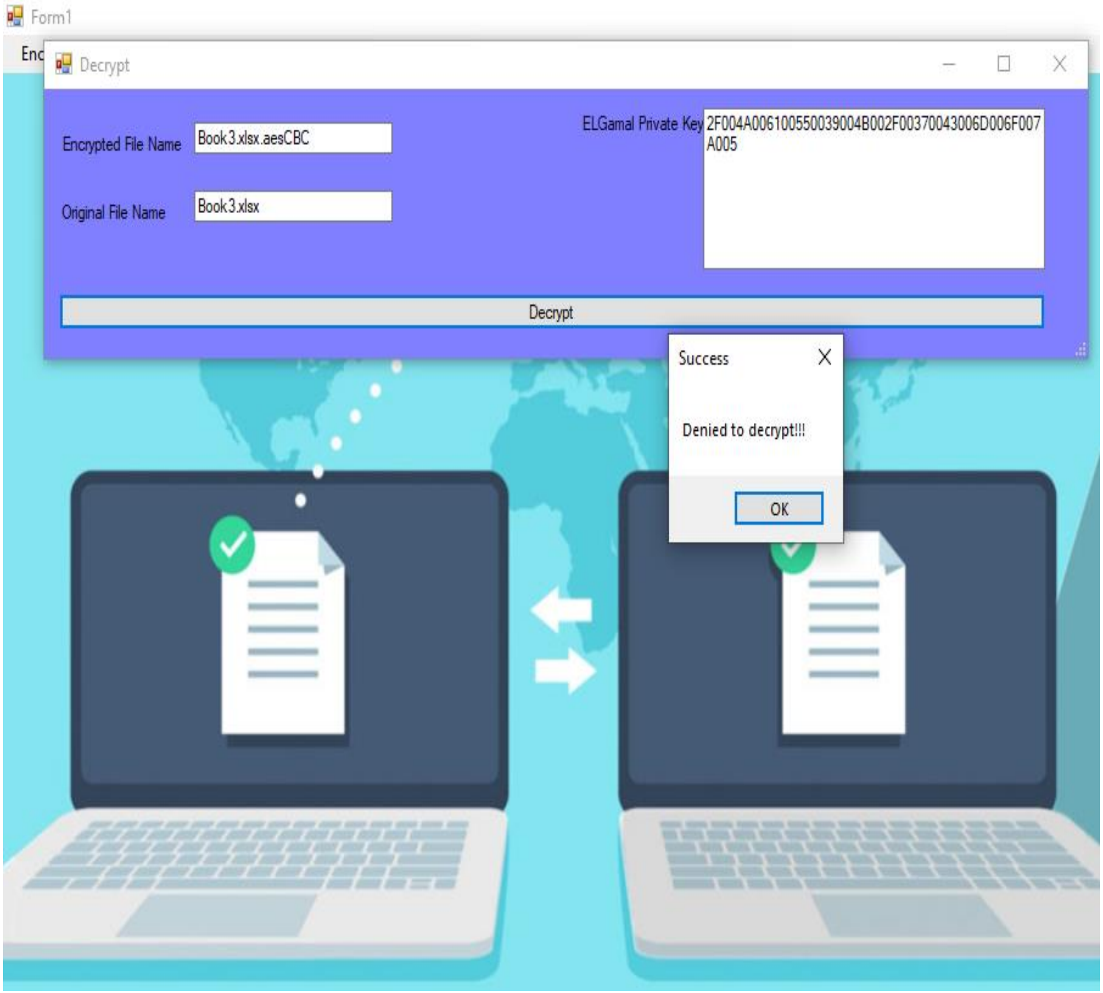
Original File Name Book3.xlsx

ELGamal Private Key 2F004A00610055003900 4B002F00370043006D006F007A0051

File Decryption is successful

Figure 4.11: Successful Message Decryption

At the point when the recipient decode the got encoded succeed record, in the event that the Elgamal key is right the beneficiary get the unscrambled succeed document which displayed in figure 4.11.



Encrypted File Name: Book3.xlsx.aesCBC

Original File Name: Book3.xlsx

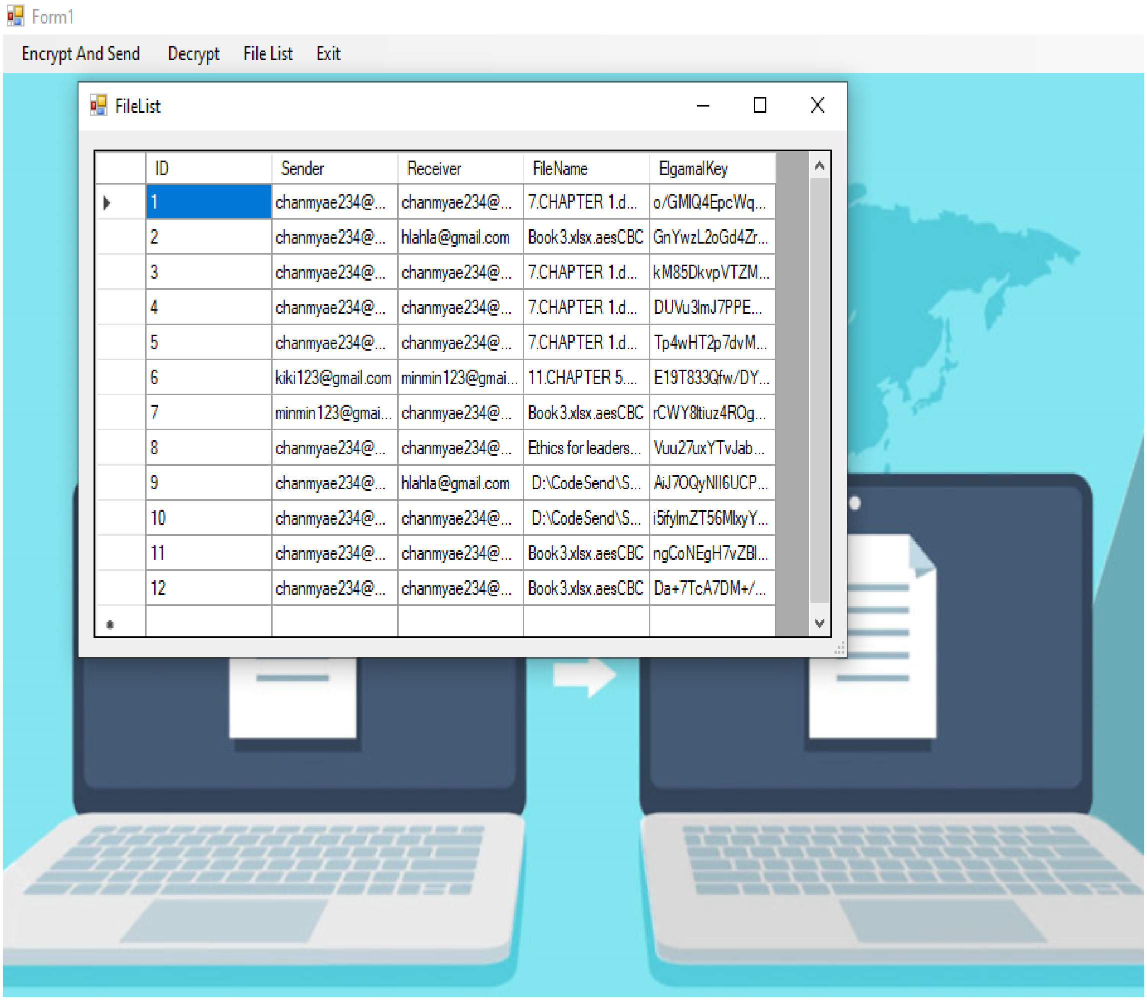
ELGamal Private Key: 2F004A006100550039004B002F00370043006D006F007A005

Success

Denied to decrypt!!!

Figure 4.12: Denied Message Decryption (For Excel File)

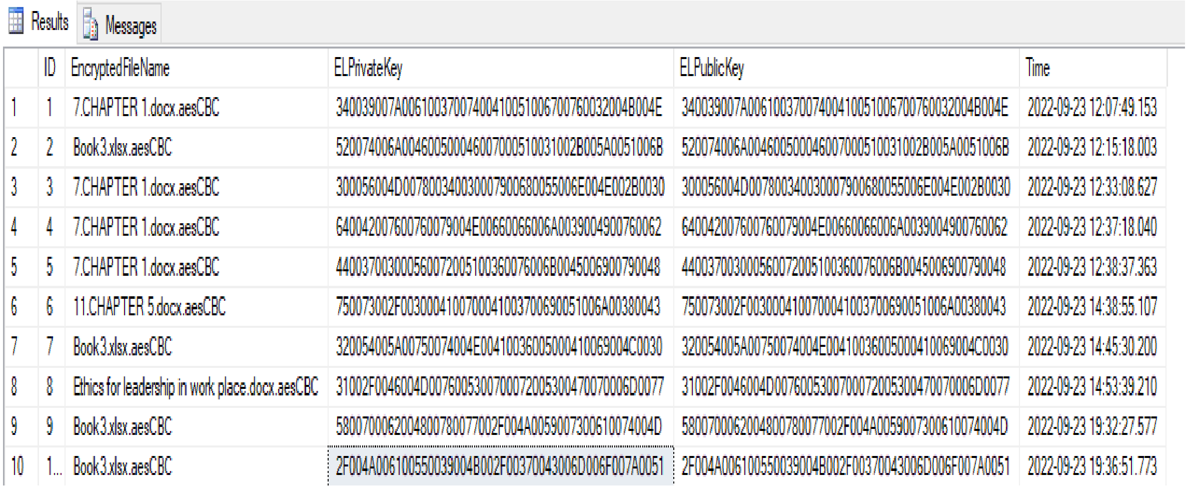
At the point when the recipient is decode the encoded succeed record, assuming the Elgamal Private Key is mistaken, the message box show the beneficiary can't the scrambled document which displayed in figure 4.12.



	ID	Sender	Receiver	FileName	ElgamalKey
▶	1	chanmyae234@...	chanmyae234@...	7.CHAPTER 1.d...	o/GMIQ4EpcWq...
	2	chanmyae234@...	hlahla@gmail.com	Book3.xlsx.aesCBC	GnYwzL2oGd4Zr...
	3	chanmyae234@...	chanmyae234@...	7.CHAPTER 1.d...	kM85DkvpVTZM...
	4	chanmyae234@...	chanmyae234@...	7.CHAPTER 1.d...	DUVu3lmJ7PPE...
	5	chanmyae234@...	chanmyae234@...	7.CHAPTER 1.d...	Tp4wHT2p7dvM...
	6	kiki123@gmail.com	minmin123@gmai...	11.CHAPTER 5....	E19T833Qfw/DY...
	7	minmin123@gmai...	chanmyae234@...	Book3.xlsx.aesCBC	rCWY8ltiuz4ROg...
	8	chanmyae234@...	chanmyae234@...	Ethics for leaders...	Vuu27uxYTvJab...
	9	chanmyae234@...	hlahla@gmail.com	D:\CodeSend\S...	AiJ7OQyNlI6UCP...
	10	chanmyae234@...	chanmyae234@...	D:\CodeSend\S...	i5fylmZT56MlxyY...
	11	chanmyae234@...	chanmyae234@...	Book3.xlsx.aesCBC	ngCoNEgH7vZBl...
	12	chanmyae234@...	chanmyae234@...	Book3.xlsx.aesCBC	Da+7TcA7DM+/...
*					

Figure 4.13: File List By AES-CBC

The file list show the shipper records, the recipient records and send document names from the source to the collector and mystery Elgamal key as displayed in figure 4.13.

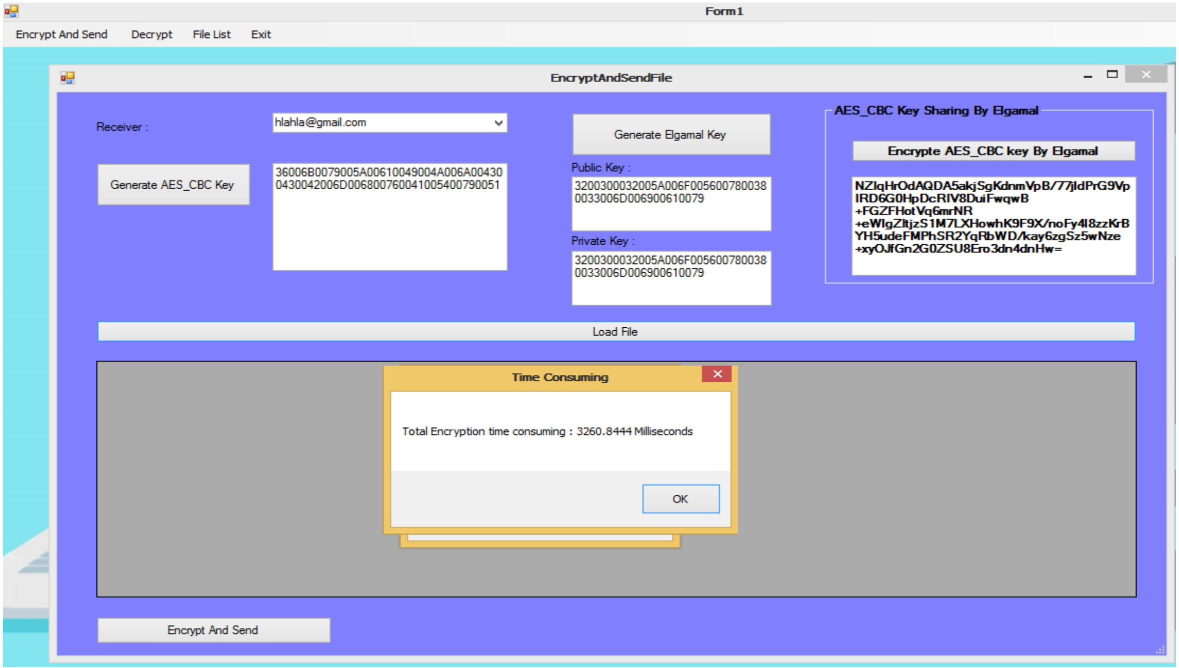


	ID	EncryptedFileName	ELPrivateKey	ELPublicKey	Time
1	1	7.CHAPTER 1.docx.aesCBC	340039007A0061003700740041005100670076003200 4B004E	340039007A00610037007400410051006700760032004B004E	2022-09-23 12:07:49.153
2	2	Book3.xlsx.aesCBC	520074006A00460050004600700051003100 2B005A0051006B	520074006A004600500046007000510031002B005A0051006B	2022-09-23 12:15:18.003
3	3	7.CHAPTER 1.docx.aesCBC	300056004D0078003400300079006800 55006E004E002B0030	300056004D00780034003000790068005 5006E004E002B0030	2022-09-23 12:33:08.627
4	4	7.CHAPTER 1.docx.aesCBC	64004200760076007900 4E00660066006A003900490076 0062	640042007600760079004E00660066006A0039004900760062	2022-09-23 12:37:18.040
5	5	7.CHAPTER 1.docx.aesCBC	4400370030005600720051003600760 06B004500690079 0048	44003700300056007200510036007600 6B0045006900790048	2022-09-23 12:38:37.363
6	6	11.CHAPTER 5.docx.aesCBC	750073002F00300041007000410037006900 51006A00380043	750073002F003000410070004100370069005100 6A00380043	2022-09-23 14:38:55.107
7	7	Book3.xlsx.aesCBC	320054005A00750074004E0041003600500041006900 4C0030	320054005A00750074004E00410036005000410069004C0030	2022-09-23 14:45:30.200
8	8	Ethics for leadership in work place.docx.aesCBC	31002F0046004D00760053007000720053004700 70006D0077	31002F0046004D0076005300700072005300470070006D0077	2022-09-23 14:53:39.210
9	9	Book3.xlsx.aesCBC	580070006200480078007 7002F004A0059007300610074004D	5800700062004800780077002F004A0059007300610074004D	2022-09-23 19:32:27.577
10	1...	Book3.xlsx.aesCBC	2F004A00610055003900 4B002F0037004300 6D006F007A0051	2F004A006100550039004B002F00370043006D006F007A0051	2022-09-23 19:36:51.773

Figure 4.14: Database Design By AES-CBC

The ElGamal Public key, Private key and Time include in the database design as shown in figure 4.14.

4.5 System Evaluation by Timestamp



Receiver : hlahla@gmail.com

36006B0079005A00610049004A006A00430
0430042006D00680076004100540079005 1

Public Key :
3200300032005A006F005600780038
0033006D006900610079

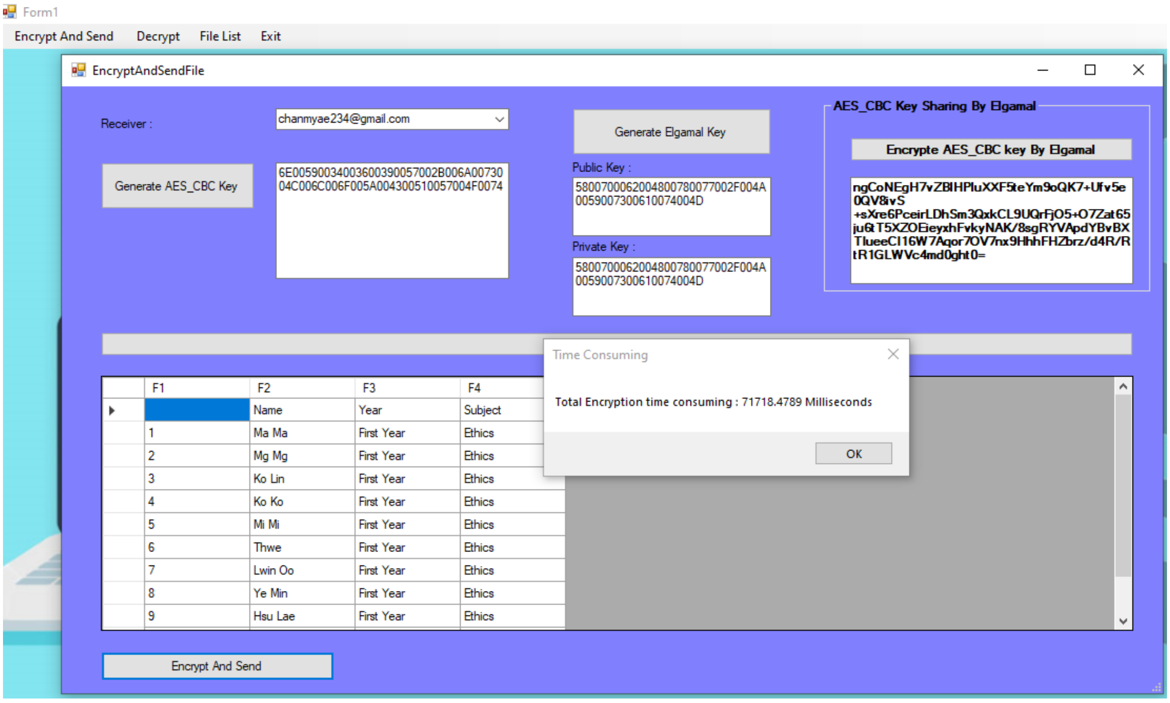
Private Key :
3200300032005A006F005600780038
0033006D006900610079

NZIqHrOdAQDA5akjSgKdnmVpB/77jldPrG9Vp
IRD6G0HpDcRIV8DuiFwqwB
+FGZFHotVq6mrNR
+eWlgZltjzS1M7LXHowhK9F9X/noFy4l8zzKrB
YH5udeFMPhSR2YqRbWD/kay6zgSz5wNze
+xyOJfGn2G0ZSU8Ero3dn4dnHw=

Time Consuming

Total Encryption time consuming : 3260.8444 Milliseconds

Figure 4.15: Time Consuming Monitoring (For Document File)



Receiver : chanmyae234@gmail.com

6E0059003400360039005 7002B006A00730
04C006C006F005A0043005100570 04F0074

Public Key :
58007000620048007800 77002F004A
0059007300610074004D

Private Key :
58007000620048007800 77002F004A
0059007300610074004D

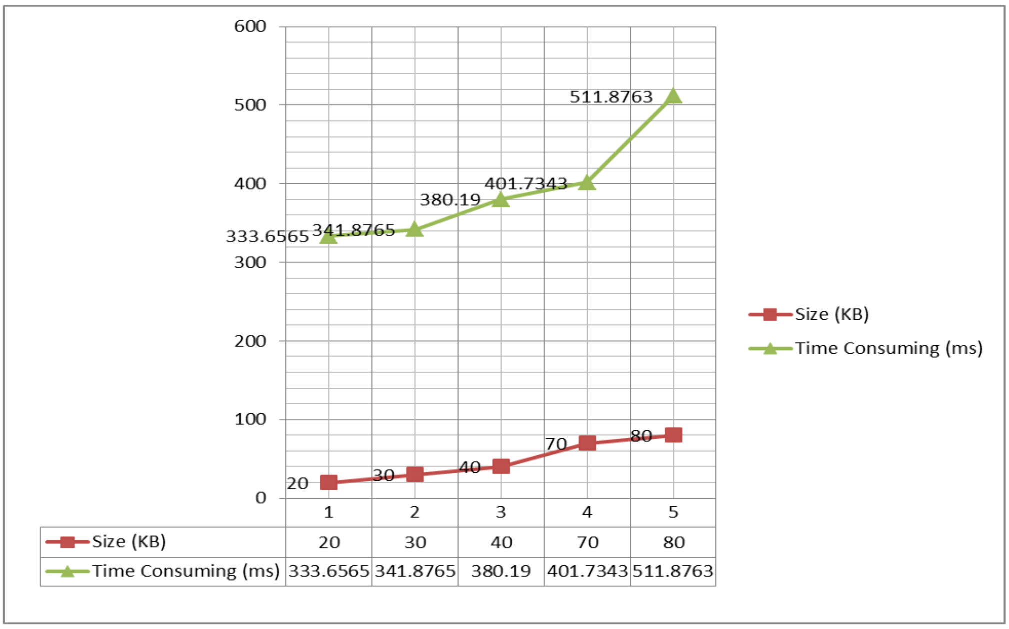
ngCoNEgH7vZBIHPluXXF5teYm9oQK7+Ufv5e
0QV8ivS
+sXre6PceirLDhSm3QxkCL9UQrFjO5+O7Zat65
ju6tT5XZOEieyxhFvkyNAK/8sgRYVApdYBvBX
TlueeCl16W7Aqor7OV7nx9HhhFHZbrz/d4R/R
tR1GLWVc4md0ght0=

F1	F2	F3	F4
	Name	Year	Subject
1	Ma Ma	First Year	Ethics
2	Mg Mg	First Year	Ethics
3	Ko Lin	First Year	Ethics
4	Ko Ko	First Year	Ethics
5	Mi Mi	First Year	Ethics
6	Thwe	First Year	Ethics
7	Lwin Oo	First Year	Ethics
8	Ye Min	First Year	Ethics
9	Hsu Lae	First Year	Ethics

Time Consuming

Total Encryption time consuming : 71718.4789 Milliseconds

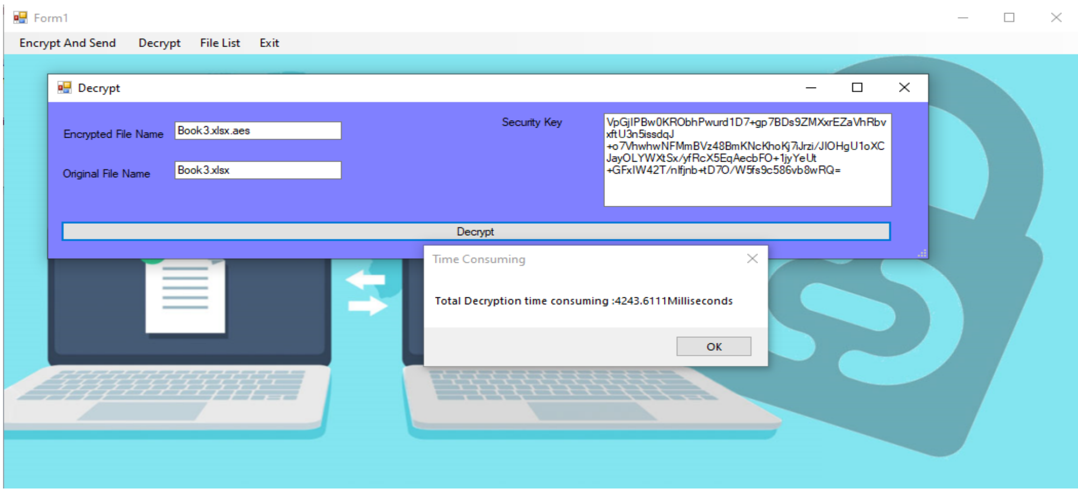
Figure: 4.16: Encryption Time Consuming Monitoring (For Excel File)



	1	2	3	4	5
Size (KB)	20	30	40	70	80
Time Consuming (ms)	333.6565	341.8765	380.19	401.7343	511.8763

Table 4.1: Time Consuming Analysis Table (Encryption Time)

This section will discuss the secure data sharing in time consuming analysis point of view. This system will explore each execution time as shown in Figure6. Different sizes of files are also processed and analyzed the various time values as shown in table 4.1. In table 4.2, five different sizes of files are tested and time consuming is shown in graph.



Encrypted File Name: Book3.xlsx.aes

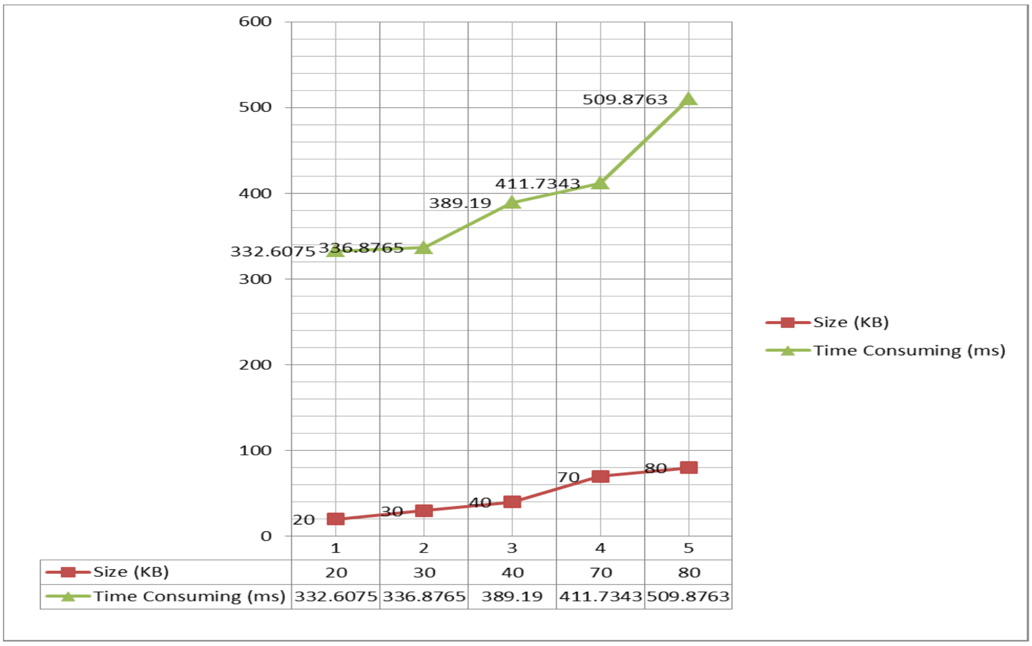
Original File Name: Book3.xlsx

Security Key: VpGjIPBw0KRObhPwurd1D7+gp7BDs9ZMXxrEZaVhRbv
xftU3n5issdqJ
+o7VhwhwNFMmBVz48BmKNcKhoKj7iJrzi/JIOHgU1oXC
JayOLYWXtSx/yfRcX5EqAecbFO+1jyYeUt
+GFxIW42T/nlfjnb+tD7O/W5fs9c586vb8wRQ=

Total Decryption time consuming :4243.6111Milliseconds

Figure 4.17: Decryption Time Consuming Monitoring (For Excel File)

Based on table 4.1 and table 4.2, encryption and decryption time consuming are not quite different and times within the reasonable and acceptable to use the system for secure file sharing.



	1	2	3	4	5
Size (KB)	20	30	40	70	80
Time Consuming (ms)	332.6075	336.8765	389.19	411.7343	509.8763

Table 4.2: Time Consuming Analysis Table (Decryption Time)

CHAPTER 5
CONCLUSION, LIMITATION AND FURTHER EXTENSION

The most popular block cipher modes of operation on AES are thoroughly compared in the proposed system in terms of encryption time, decryption time, and throughput for.doc and.xlsx file encryption. The proposed system uses the CBC operating mode. The block cipher may also be applied to a stream of plaintext using different modes of operation, which would increase the algorithm's effectiveness. This system can provide a service for secure file sharing by using AES on CBC mode. For secure key sharing purpose, this system will also be used ElGamal encryption algorithm to encrypt the AES-CBC's symmetric key. The proposed system is intended to provide the secure data sending for file sharing system in campus environment.

5.1 Limitation and Further Extension

The proposed system is based on file sharing system for secure passing. This system encrypted the secure file and decrypt by using AES-CBC. This system only emphasize on the .doc and .xlsx file encryption. This system can be extended for the data securing passing system such as encryption for data shipping system which include data compression for light weighted data transmission.

REFERENCES

[1] A. Ramesh and A. Suruliandi, “Performance analysis of encryption algorithms for Information Security,” in 2013 International Conference on Circuits , Power and Computing Technologies (ICCPCT),. IEEE, 2013, pp. 840–844.

[2] A. Desai, K. Ankalgi, H. Yamanur, and S. S. Navalgund, “Parallelization of AES algorithm for disk encryption using CBC and ICBC modes,” in Fourth International Conference on Computing , Communications and Networking Technologies (ICCCNT), 2013. IEEE, 2013, pp. 1–7. 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)

[3] Dobre Blazhevski Adrijan Bozhinovski Biljana Stojchevska Veno Pachovski, “ MODES OF OPERATION OF THE AES ALGORITHM” , The 10th Conference for Informatics and Information Technology (CIIT 2013)

[4] D. Hook, Beginning cryptography with Java. John Wiley & Sons, 2005.

[5] D. S. A. Elminaam, H. M. Abdual-Kader, and M. M. Hadhoud, “Evaluating The Performance of Symmetric Encryption Algorithms.” IJ Network Security, vol. 10, no. 3, pp. 216–222, 2010.

[6] G. Kumar, M. Rai, and G.-s. Lee, “Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement,” International Journal of Security and Its Applications, vol. 6, no. 1, pp. 57–72, 2012.

[7] J. Thakur and N. Kumar, “DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis,” International journal of emerging technology and advanced engineering, vol. 1, no. 2, pp. 6–12, 2011.

[8] K. V. Pradeep, V. Vijayakumar,1 and V. Subramaniyaswamy, “An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment”, Journal of Computer Networks and Communications Volume, 2019.

[9] K.-T. Huang, J.-H. Chiu, and S.-S. Shen, “A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Ciphers,” International Journal of Network Security & Its Applications (IJNSA), vol. 5, no. 1, p. 19, 2013.

[10] K. R. Saraf, V. P. Jagtap, and A. K. Mishra, “Text and Image Encryption Decryption Using Advanced Encryption Standard,” International Journal of Emerging Trends & Technology in Computer Science, 2014.

[11] N. Singhal and J. Raina, “Comparative Analysis of AES and RC4 Algorithms for Better Utilization,” International Journal of Computer Trends and Technology, vol. 2, no. 6, pp. 177–181, 2011.

[12] Razvi Doomun*, Jayramsingh Doma, “AES-CBC Software Execution Optimization”, Sundeep Tengur Computer Science and Engineering, University of Mauritius, 2014.

[13] P. Mahajan and A. Sachdeva, “A study of encryption algorithms aes, des and rsa for security,” Global Journal of Computer Science and Technology, vol. 13, no. 15, 2013.

[14] Sultan Almuhammadi and Ibraheem Al-Hejri, “A Comparative Analysis of AES Common Modes of Operation”, 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)

[15] W. Stallings, Cryptography and network security: principles and practices. Pearson Education India, 2006.

PUBLICATION

[1] Chan Myae Thu and Amy Tun, “Securing File Sharing Using AES-CBC Authenticated Encryption”, parallel and soft computing PSC, University of Computer Studies, Yangon, Myanmar, 2022.