INTRODUCTION

1.1 BACKGROUND:

As the computers and networked systems increases in the world of today, the need for increased data security also becomes necessary and important. The development of computer network system has exposed many networks to various kinds of authentication threats and with these exposures; one can see that the need for increased network and data security is vital and important in every organization.

The security may include identification, authentication and authorization of user in a network environment. Some cryptography technique may be used to solve all these problems.

Cryptography technique has reduced unauthorized access of data. Encrypted data may be stored in to file. Then authorized person are supposed to decrypt this data with the help of some keys.

1.2 OBJECTIVES

The main objective of our project is to encrypt or decrypt the any files for personal and professional security. Encryption and Decryption protects privacy of our documents and sensitive files by encrypting them using Advanced Encryption Standard (AES) algorithm to provide high protection against unauthorized data access.
In today's world the networking plays a very important role in our life. Most of the activities occur through the network. For the safe and secured exchange of information, we need to have security. The encryption has very wide applications for securing data.Encryption refers to set of algorithms, which are used to convert the documents and any files to code or the unreadable form of files, and provides privacy. To decrypt the file to receiver uses the "key" for the encrypted files.

If you want to send sensitive information via email, simply paste the encrypted text or any files into your email or attach the encrypted file.

All the recipient has to do is to decrypt your text or any file. Encryption and Decryption works with text information and any files. Just select what you want to encrypt, and Encryption and Decryption software helps you keep documents, private information and files in a confidential way.

The project has the following objectives

1) Storing important information in encrypted form ensuring security.

2) We can prevent information loss when system crashes occurred.

3) The information will be recovered from the backup data.

4) Enhancing efficiency of data retrieval.

5) File Sending.

6) Better accuracy and improved consistency.

7) Help facility will be provided.

8) To understand and improve the computer data security through encryption of data.

9) To enhance the integrity of data.

10) To develop a platform to complement physical security.

1.3 PURPOSE AND SCOPE

1.3.1 PURPOSE:

In today's world most of the communication is done using electronic media. Data security plays vital role in such communication. Hence, there is a need to protect data from malicious attacks. This can be achieved by cryptography. The earlier encryption algorithm is Data Encryption Standard (DES) which has several loopholes such as small key size and sensible to brute force attack etc. These loopholes overcome by a new algorithm called as Advanced Encryption Standard Algorithm.

1.3.2 SCOPE:

The scope of our project is presently specific. Both the sender and the receiver must have this software installed on their systems to encrypt or decrypt and compress or decompress the files transmitted between them. This includes all the users who want to interact electronically, whether it is through emails, sending a files etc.through local area network in order to keep their private information confidential.

- Each step is clearly stated and user will not face any ambiguity in using the software.
- The software provides clarity in its functionality even to naïve users.
- No complexity is involved.
- The various scope which cryptographic algorithms guarantees certain level of security, confidentiality and integrity of data.

2 SURVEY OF TECHNOLOGIES:

This project can be developed in any language as here we uses AES Encryption Algorithm and since Encryption algorithms can be encoded in any language so does this project, so languages such as Java, C++ or python anyone can be used but here **python is the best fit for this project due to certain reasons:**

1) Built In libraries for Numerical Computation:
Being an open source and platform independent python provides a greate variety of libraries for usual and complex both type of tasks, it has very effecient libraries regarding the Numerical Computations entities which gives us liberty to use them rather than buiding each thing from scratch.

2) Highly Object Oriented:
Python is one of the popular object oriented programming language in the recent past and at present also,which helps us in using the object oriented methods and concepts quite easily in this language.

3) Faster rate of Development:
Being an open source and very popular language, python is flourishing like nothing else and which provides us facilites to nuture our code and modify it to the best level, which can be easily done in this language.

4) Interpreted Than Compiled:
Since python is interpreted by its interpreter rather than compiled which makes it user friendly for the detection of errors in codes whether it would be a logical or syntax error, both can be easily rectified in this language.

3 REQUIREMENTS AND ANALYSIS

3.1 PROBLEM DEFINITION:

Project Mission

The aim of our project is to develop software named "ENCRYPTION SYSTEM". The project encrypts and decrypts the any files using Advanced Encryption Standard (AES) algorithm to maintain the security and integrity of data and information and to provide high protection against unauthorized data access.

Target

Our target is the common man who wants to interact client and server, whether it is through messages, documents and any files etc. Through network via file sending sensitive messages or documents over the network is very dangerous.So, our project helps him to interact in a safe and secure manner in order to keep their private information confidential.

Target Users

The main target users of our project are the people who transmit confidential information network via file sending sensitive messages or documentst hrough the client server interaction.

Scope and Key Elements

The scope of our project is presently specific. Both the sender and the receiver must have this software installed on their systems to encrypt/decrypt and compress/decompress the files transmitted between them. The system provides the security and integrity of data or information.

- It will provide a more clear and non-ambiguous description of the functions.
- The system is highly user friendly.
- It uses secret keys for encryption and decryption.
- The software provides clarity in its functionality even to naïve users.

Analysis is the detailed study of the various operations performed by a system and their relationships within and outside the system. System analysis is an approach to study the system and find a solution. It provides as frame work for visualizing the organizational facts that operate on a system. The aspect of analysis is defining the boundaries of the system and determining whether or not a candidate system should consider.

During the analysis the data are collected from the available resources for analysis. Information from the existing system, dataflow diagram, on site observations and interviews are the various tools used during the analysis to collect information. The natural problem solving process consists of the following steps.

1) The identification of the problem situation that needs to be solved.

2) Defining the problem.

3) Defining the desired outcome.

4) Provide possible alternative solution.

5) Identifies and selects the best one among them.

Identification of Need

This network project aims to achieve storing of most important information in encrypted form. They rely on a secret piece of information called the key. Hacker's objective is to obtain the key from the communication. The various scope which cryptographic algorithms guarantees certain level of security, confidentiality and integrity of data.

There is great need for encryption, authentication techniques, user identification and passwords. These will all protect your computer from damage or from hackers (people who gain access to your Computer and then steal your Data).

Encryption is only one method which can be used when you want to be able to protect your computer from harm and hackers. Encryption is when you put a secret key or password on your work that will then transform your data into an unreadable file if you don't have the secret key and password. It is best to encrypt something that you will transfer over the network because it has high chances of being stolen because it is rather easy when it is being transferred so much from computer to computer. Now the best way to transfer this secret key is face to face because otherwise then the secret key might be taken by someone else will you transfer it across the network. Encryption is a pretty easy thing to do but if one of your documents really needs to be encrypted for its safety it is extremely easy to find software to help you increase your security.

Feasibility study

After investigation it is essential to determine whether the project is feasible or not. In feasibility study is tested whether the system to be developed would be able to accomplish its task on the working grounds. Its impact was also found to be not adverse. It was found that the user's requirements would be met and the resources would be used in an effective manner. In feasibility study the important aspects related to the project were considered like the problem definition and the process for solution. The cost and benefit analysis was also done.Essential features involved in the feasibility analysis are:-

- Behavioral Feasibility
- Economic Feasibility

- Technical feasibility
- Operational Feasibility

Behavioral Feasibility

An estimate should be made of how strong a reaction the users is likely to have toward the development of a new system. It is common that the new system requires special effort to educate, sell and train the users. But in the case of the Virtual Drive, anyone who has a basic knowledge of computer can easily work with this system so the users do not feel any difficult with this, so they can accept the system without any willingness.

Technical Feasibility

Technical feasibility revolves around the technical support of the project. The main infrastructure of the project included the project labs in the college campus. The systems there were easily able to absorb the new software being installed. The project thus was technically feasible. The equipment and the software produced no problem. The project's technical requirements were met. The project could be made to work correctly, fulfilling its task, with the existing software and personnel.

Economic Feasibility

The project developed, Encryption and Decryption was within budget and producing the desired results. The labor or the human ware consisted of the four group members of our project. The output consisted of getting the desired results. Thus with the consideration of the inputs, the outputs were achieved successfully. The project was within limit. The inputs didn't overdo the outputs.

Operational Feasibility

Operational Feasibility aims to determine the impact of the system on the users. The system developing has an influence on its users. Our system "Advanced Encryption System" was new for them but it was simple enough for any naïve person to understand. The evolution of this new system required no special training for the users. Encryption and Decryption was found to be feasible in this regard. The system developed would be user friendly and no complexities would be involved in its functionalities.

3.2 REQUIREMENTS SPECIFICATION

The main aim of preliminary analysis is to identify the problem. First, need for the new or the enhanced system is established. Only after the recognition of need, for the proposed system is done then further analysis is possible.

Existing System

In the existing system, the encrypted key is send with the document; any user can view the encrypted document with that key. It means the security provided for the encryption is not handled properly. And also the Key byte (encrypted key) generate with random byte. Without the user interaction the Key byte is generated. As observed the current encryption/decryption software's doing the encryption and decryption task are all very complicated in their functionality. The method of encryption/decryption and key generation of current system for a new user to understand is complex in nature.

Drawbacks

Some of the drawbacks are:

1. Lack of security

2. Key byte is generated without user interaction

Proposed System

The proposed system is quiet simple to use. It is not complex in its functionalities. It is easy for a naïve user to use it.

If you want to send sensitive information via network, simply paste the encrypted file.
All the recipient has to do is to decrypt your file.Encryption and Decryption works with any information and files. Just select what you want to encrypt, and Encryption and Decryption software helps you keep documents, private information and files in a confidential way. The proposed system will help the user to reduce consuming time. The system requires very low system resources and the system will work only in network connections.

Benefits

1. Security is enhanced in well manner.
2. Users set the byte key manually.

Software Requirements Specification

Software Requirements Specification (SRS) is the starting point of the software development activity. Little importance was given to this phases in the early days of software development. The emphasis was first on coding and then shifted to design.

The purpose of this project is to demonstrate how some of the more popular encrypting algorithms. The system will allow the user to enter any files, select an encryption method, and then view the file encrypted by the selected algorithm. When an encryption method is selected, options pertaining to that specific algorithm will be displayed for the user to customize. When

the user presses the "Encrypt" button, the algorithm will then begin encrypting the files. After each calculation, a file will be displayed to the user relating to the operation that has just been performed. These files will allow the user to understand the method used in the encryption algorithm. When the algorithm is finished, the user will have the file encrypted according to the method selected and options selected.

Some of the difficulty is due to the scope of this phase. The software project is imitated by the client needs. In the beginning these needs are in the minds of various people in the client organization. The requirement analyst has to identify the requirements by tacking to these people and understanding their needs. In situations where the software is to automated a currently manuals process, most of the needs can be understood by observing the current practice.

The SRS is a means of translating the ideas in the minds of the clients (the output) into formal document (the output of the requirements phase). Thus the output of the phase is a set of formally specified requirements, which hopefully are complete and consistent, while the input has none of these properties.

Performance Requirements

The project must the end user requirements. Accuracy and fast must be imposed in the Project. The project is development as easy as possible for the sake of end user. The project has to be developed with view of satisfying the future requirements and future enhancement. The tool has been finally implemented satisfying the needs specified by the company. As per the performance is concerned this system said is performing This processing as well as tine taken to generate well reports were also even when large amount of data was used.

Security Requirements

Web application are available via network access, it is a difficult. If not possible, to limit the population of the end-user who may access the applications? In order to product sensitive connect and provide secure mode be implemented throughout the infrastructure that the supports web application and within the application itself.

Design Requirements

To create project, add base masters and masters to the project, assign behaviors to the master, create and assign behavior sets, and then apply, test and validate those behaviors. It also shows how to create and build a stencil to hold the shapes.

Quality and Reliability Requirements

A software component that is developed for reuse would be correct and contain no defects. In reality, formal verification is not carried out routinely, and defects can add to occur.However, with each reuse, defects are found eliminated, and a components qualify improve as a result. Over time the components virtually defect free.

Software reliability is defined in statically term as ”the probability of faultier-free operation of a computer program in a specified environment for specified tine”. The software quality and reliability, failure is nonconformance to software requirements. Failure can be only anything or catastrophic. One failure can be corrected within seconds while another requirements week even mouths to correct. Complicating the issue even further, the correction of the one failure may in fact result in the introduction of the errors that ultimately result in other failure.

3.3 Planning and Scheduling:

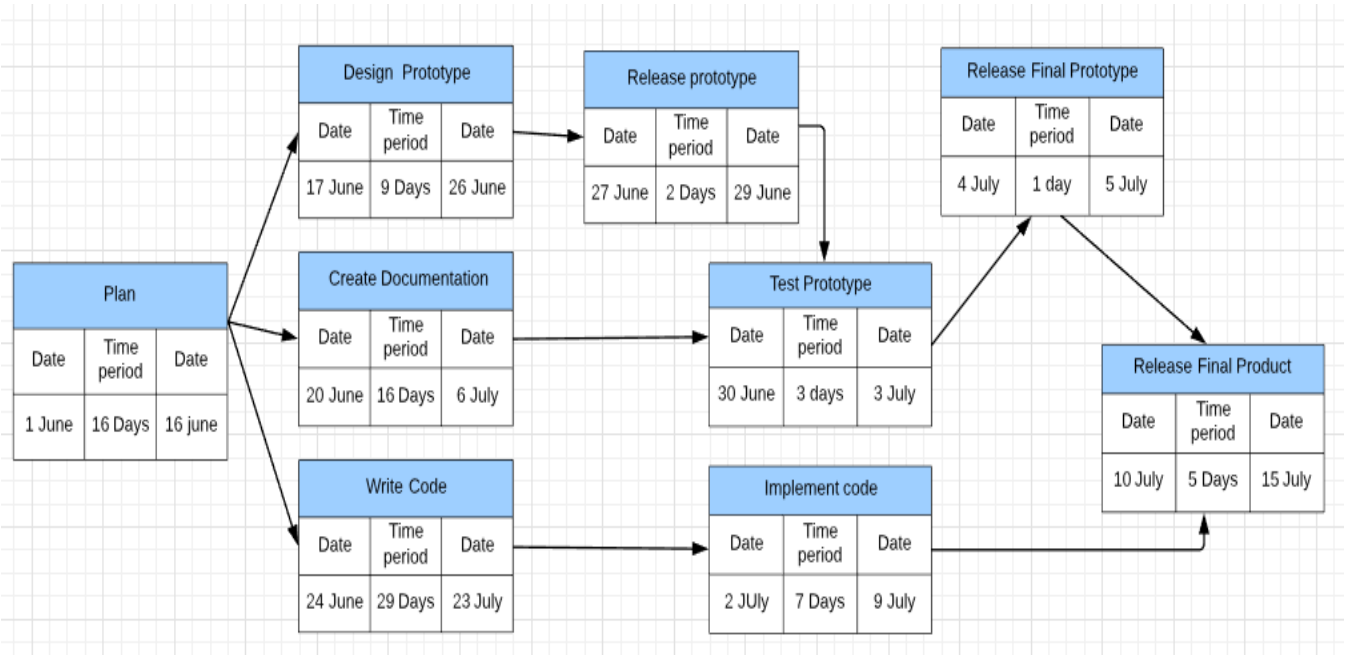
Gantt Chart

A Gantt chart is popular type of chart that illustrates a project schedule. Gantt Chart illustrates the start and finish dates of the terminal elements and summary elements of a project. Terminal element and summary comprise the work breakdown structure of the project.

Task	4Apr-30Apr	31Apr-9May	10May-12June	13June-12Jully	13Jully-18Jully	18Jully-23Jully
Develop project proposal	27 days					
Analysis		10 days				
Designing			30 days			
Coding				29days		
Unit Testing					5 days	
Implementation						5 days

Gantt Chart

Pert Chart



3.4 SOFTWARE AND HARDWARE REQUIREMENTS:

3.4.1 HARDWARE REQUIREMENTS:

Client Side	
Processor	Dual Core or above
RAM	1 GB
Disk space	500 GB
Monitor	15”
Others	Keyboard, mouse, Internet Connection

Server Side	
Processor	I3 or above
RAM	4 GB
Disk space	500 GB
Monitor	15”
Others	Keyboard, mouse, Internet Connection

3.4.2. Software Requirements:

To develop this project there are certain software requirements that needs to be fulfilled and these are as follows:

1) Anaconda Distribution 5.3.0 or higher :
This is needed to provide python version 3.6 or higher and other supporitive libraries built formachine learning and othere powerfull uses of python language.

2) Jupyter Notebook or Jupyter Lab:
It is a web based user interface, which works as an IDE for the supportive kernels, and it is needed to prepare the notes and for trying dry code runs, moreover it is a full fleged utility to work interactively with codes.

3) Visual Studio Code:
It is an Ide which is needed to help in creating effecient code files with proper extensions provided in it for python and other languages such as Html and javascript, and the whole project actual compilation would be performed here only in this project.

4) Selenium Automated Testing Suite:
This is needed for performing the Automated testing of the project developed as a whole and as well as different units of the project. Moreover for the use of selenium there is also a need of corresponding web browser driver, which is needed to bind the selenium automated testing suite to the web browser that user want to use.

5) Mathematical Computation Library 'Numpy’: They are needed for performing the task of deducing the semantic textual similarity between the two sentences and to train the developed model for the algorithims used in this project.

6) Web Browser:
This is needed to perform the testing procedure at the time of project development more specifically the elements of the web interface developed.

7) Linux OS:
since any operating system can be used for the project development but the open source linux is quite better in terms of integrating the above mentioned softwares effeciently.

8) Lucidchart:
This is a website which provides easy diagramming tool for the development UML Diagrams and other figures used in this projet at no cost.

9) Libre office:
This is an open source office package which is needed for the development of documents used in this project.

3.5 PRELIMINARY PRODUCT DESCRIPTION:

Functions

- Development of security control components for front-end systems.
- High-speed data encryption/decryption operations, password authentication, and key management for back-end system.
- For real-world applications, a complex web of software systems is required to ensure security.

Features

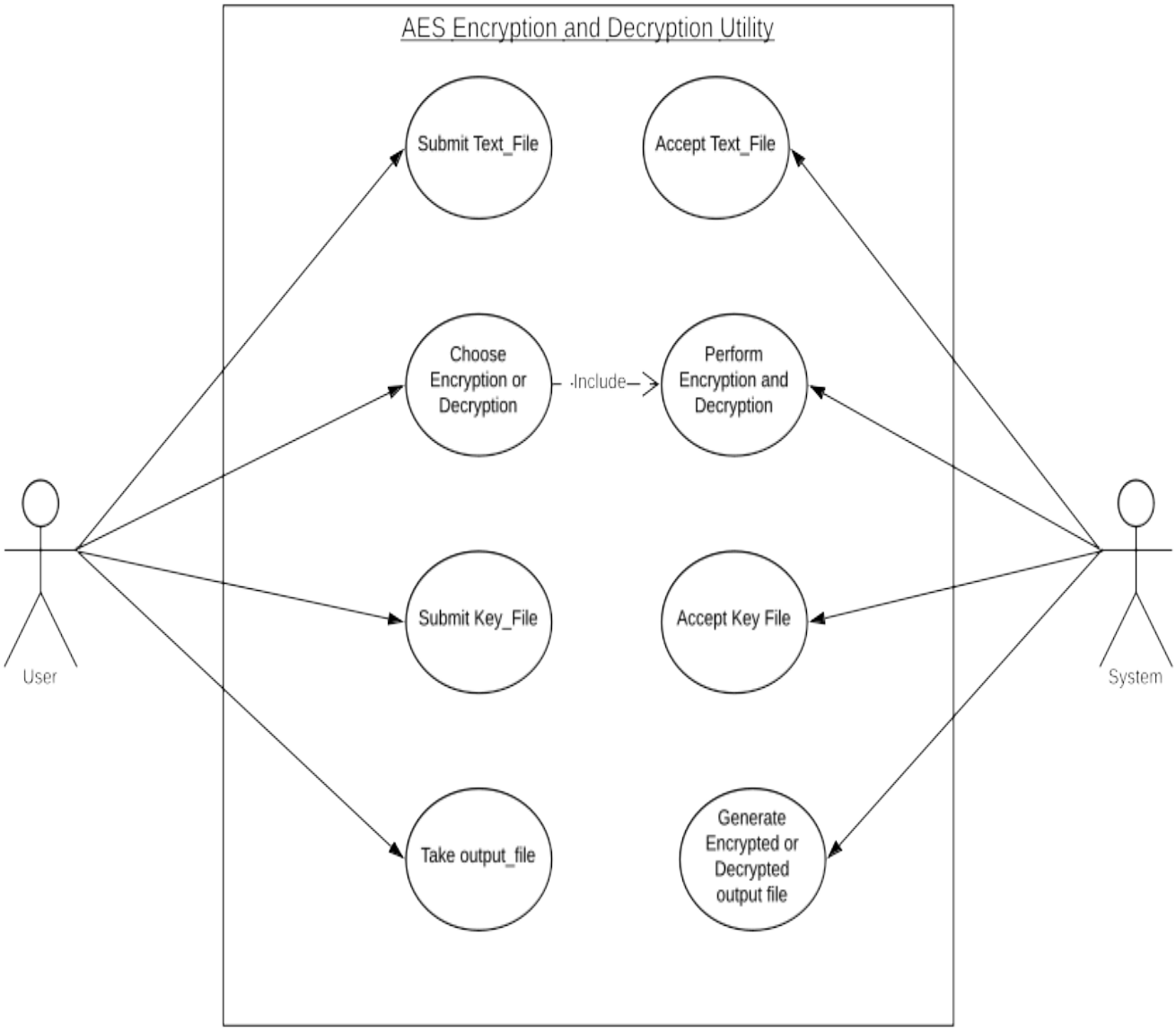
- The system is highly user friendly.
- It uses different keys (a key pair) for encryption and decryption. These algorithms are called "AES".
- The system provides security and convenience as keys never need to be transmitted or revealed to anyone.
- The system provides the integrity of data or information.
- The software provides clarity in its functionality even to naïve users.
- Network connection encryption/decryption services: Providing host encryption/decryption operations via network connection through the external security control server.
- Complete key building service: Providing complete key building and management functions, supporting multi-server key sync operations.

Benefits

In order to successfully expand the business, the security level of various application systems is enhanced to meet the requirement from authorities or organizations.

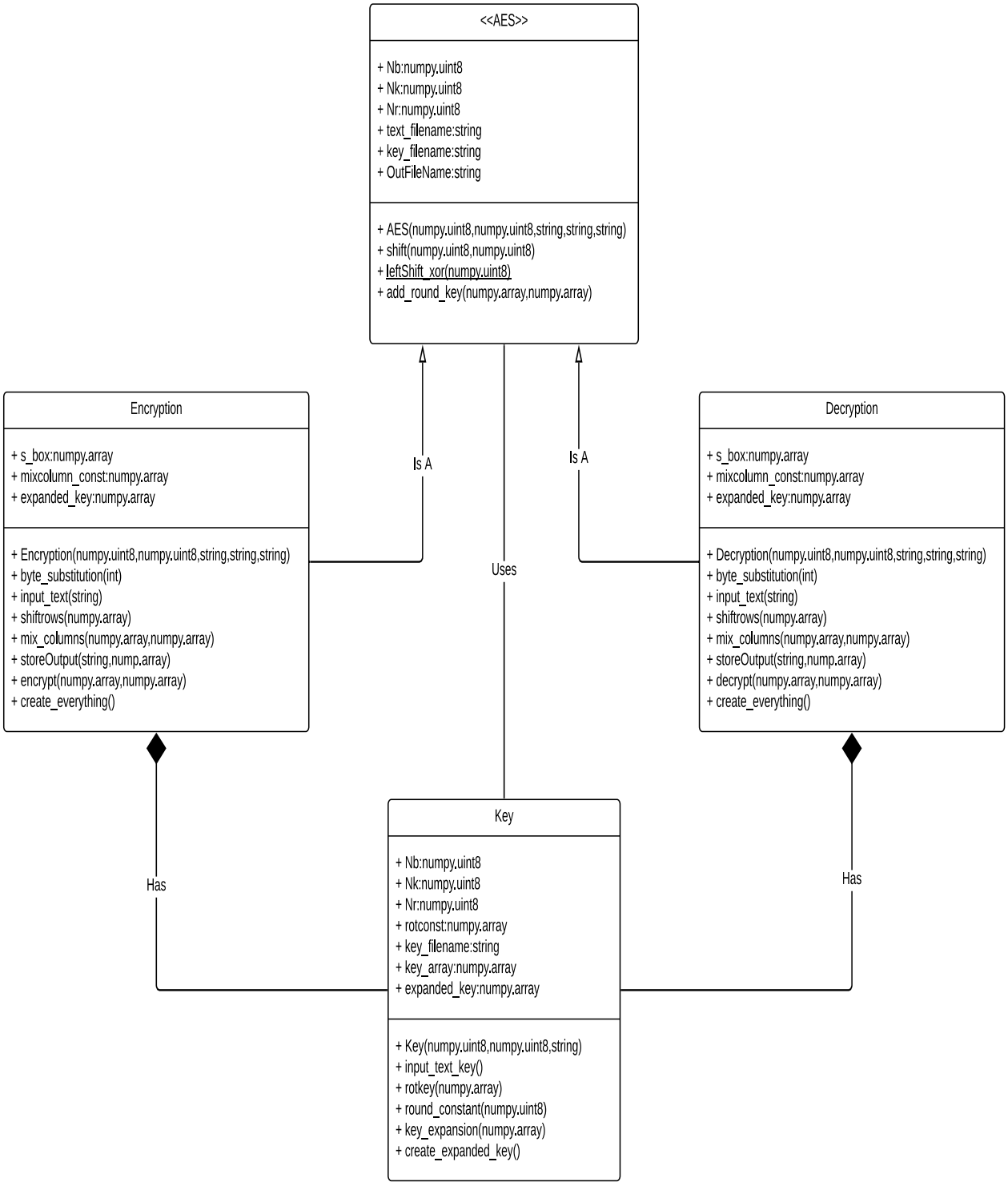
- Enhancing the security level of various application systems to prevent leakage of confidential information.
- Complying with the security specifications of various authorities and international organizations to successfully expand different businesses.

3.6 Conceptual Models:



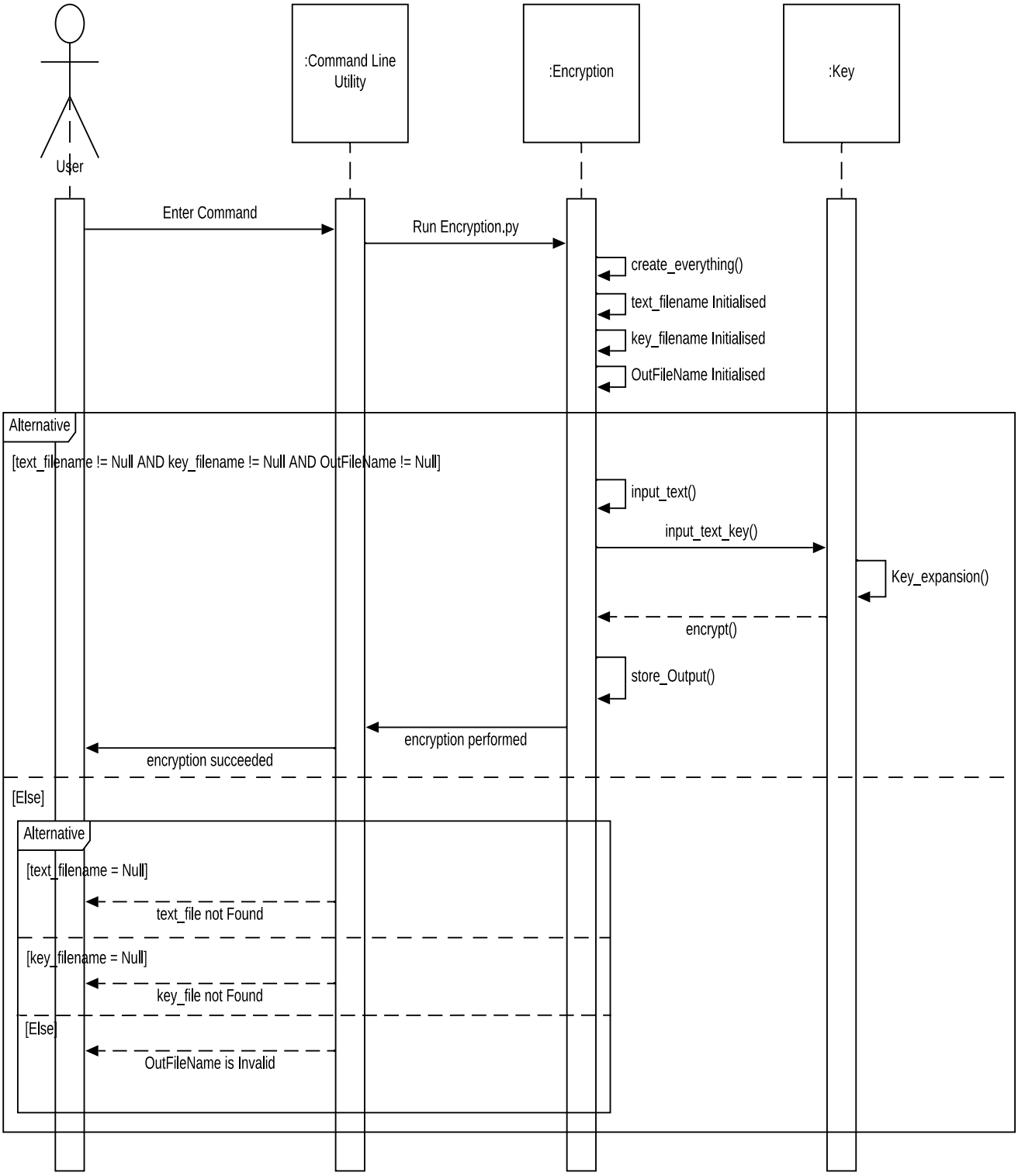
1. USE CASE DIAGRAM

Class Diagram



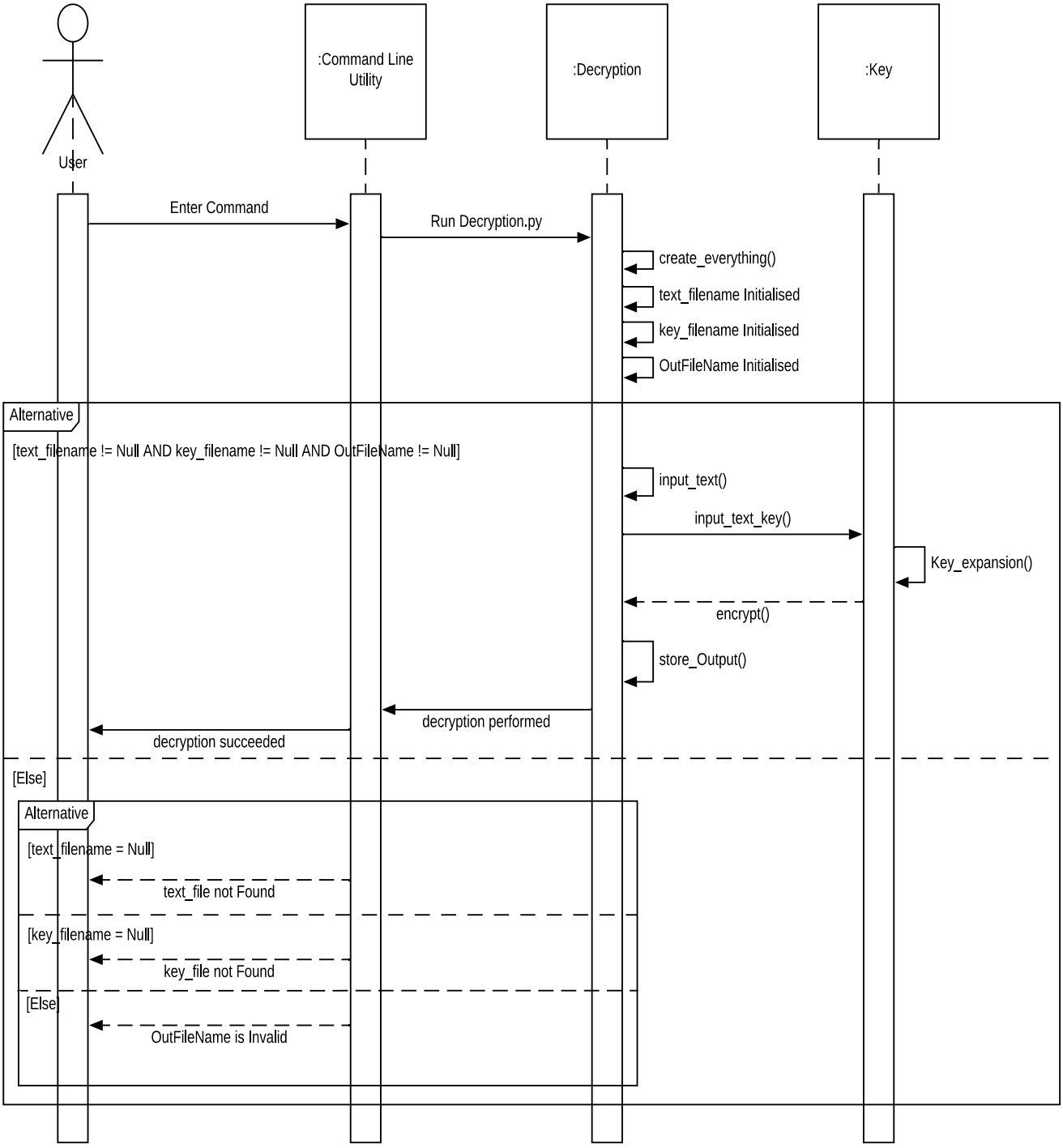
2. CLASS DIAGRAM

Encryption Sequence Diagram

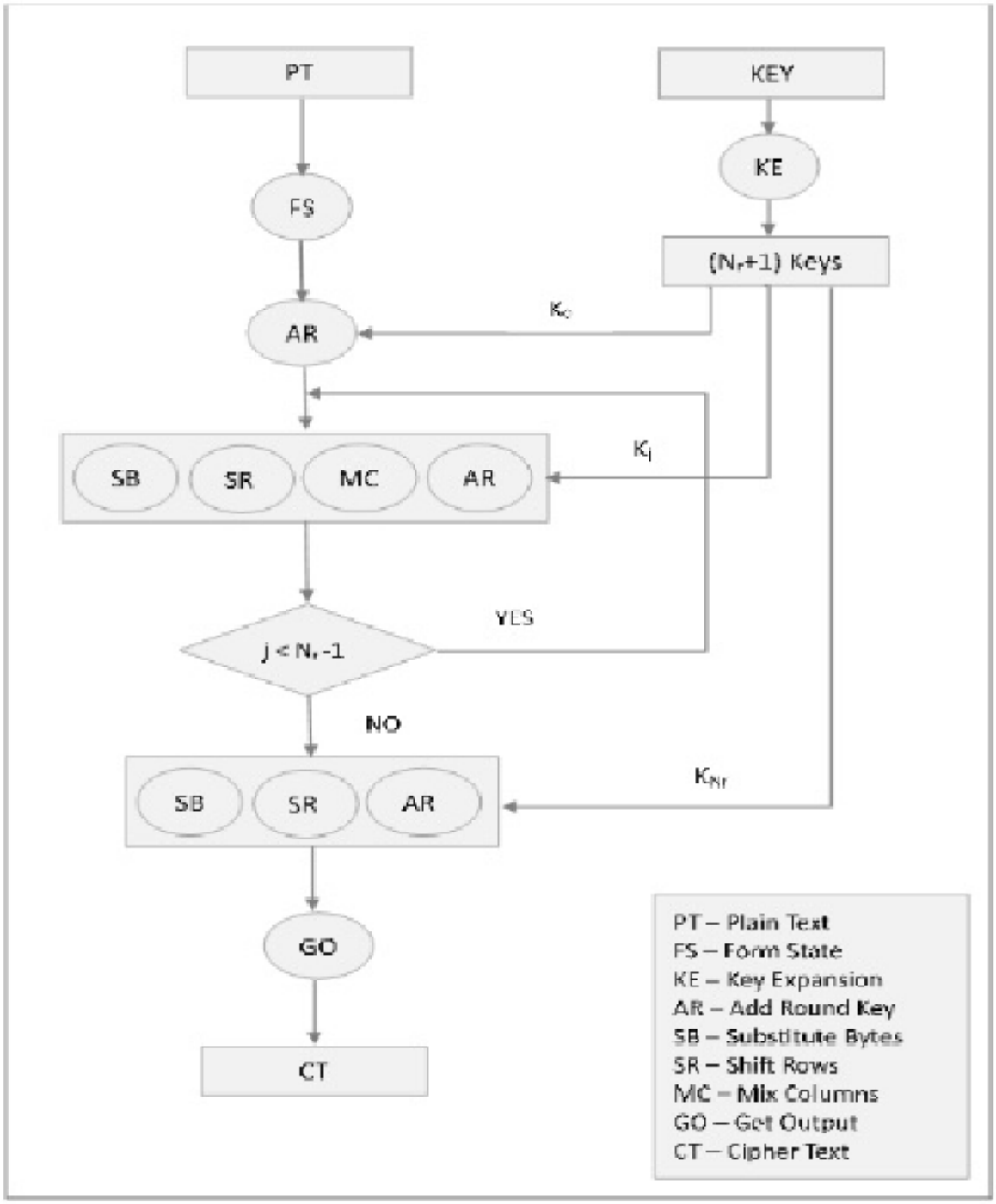


3. SEQUENCE DIAGRAM FOR FILE ENCRYPTION

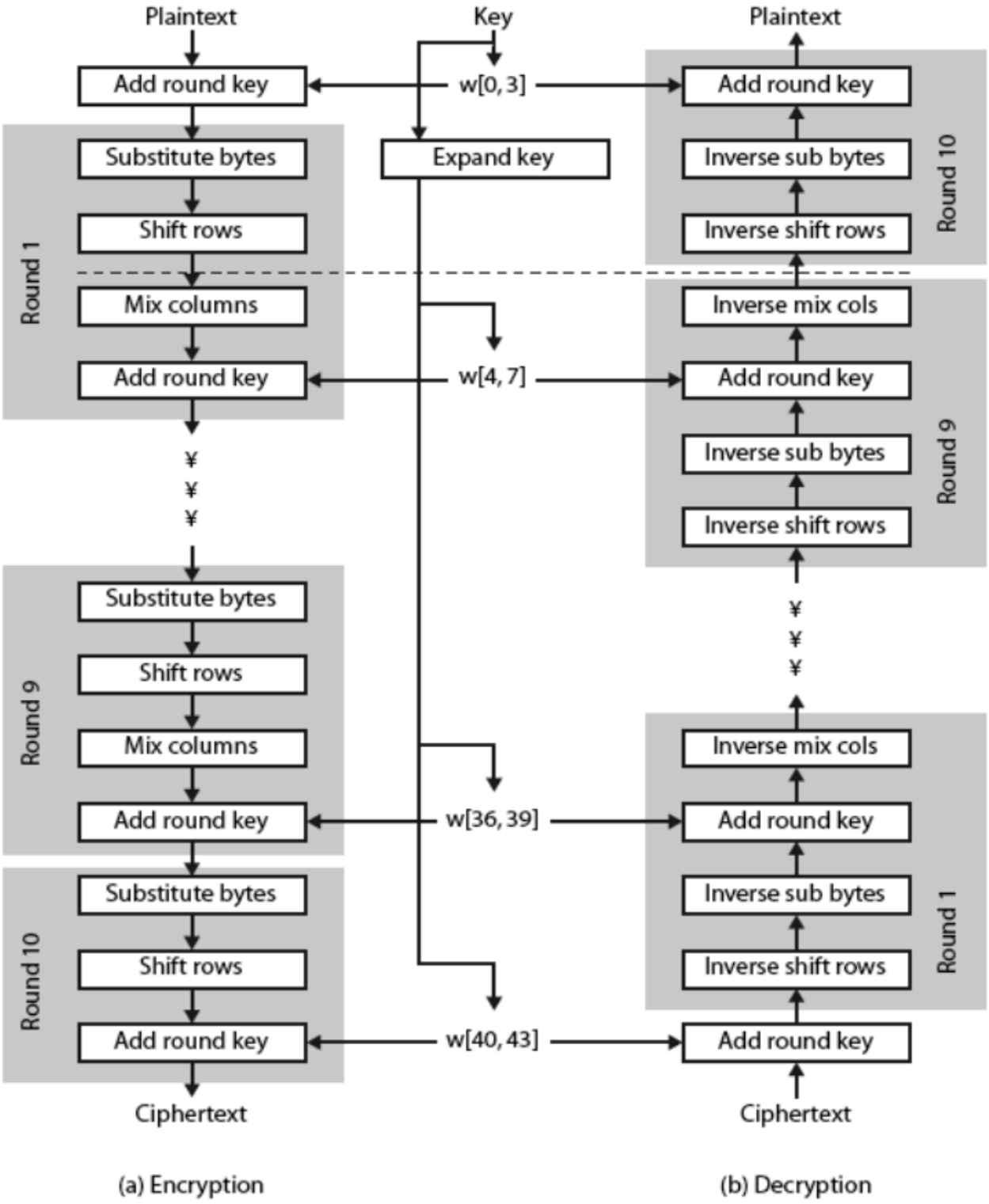
Decryption Sequence Diagram



4. SEQUENCE DIAGRAM FOR FILE DECRYPTION


PT
KEY
FS
KE
(Nr+1) Keys
AR
Kc
SB
SR
MC
AR
Ki
YES
j < Nr -1
NO
SB
SR
AR
KNr
GO
CT
PT – Plain Text
FS – Form State
KE – Key Expansion
AR – Add Round Key
SB – Substitute Bytes
SR – Shift Rows
MC – Mix Columns
GO – Get Output
CT – Cipher Text

5. FLOW CHART



6. BASIC STRUCTURE OF AES

4 References:

Abdullah, A. M., & Aziz, R. H. H. (2016, June). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm., International Journal of Computer Applications, Vol. 143, No.4 (pp. 11-17).

Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. International Journal of Computer Applications, 67(19).

Gaj, K., & Chodowiec, P. (2001, April). Fast implementation and fair comparison of the final candidates for Advanced Encryption Standard using Field Programmable Gate Arrays. In Cryptographers' Track at the RSA Conference (pp. 84-99). Springer Berlin Heidelberg.

Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India.

Yenuguvanilanka, J., & Elkeelany, O. (2008, April). Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm. In Southeastcon, 2008. IEEE (pp. 222-225).

Lu, C. C., & Tseng, S. Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on (pp. 277-285).

Mohamed, A. A., & Madian, A. H. (2010, December). A Modified Rijndael Algorithm and it's Implementation using FPGA. In Electronics, Circuits, and Systems (ICECS), 2010 17th IEEE International Conference on (pp. 335-338).

Deshpande, H. S., Karande, K. J., & Mulani, A. O. (2014, April). Efficient implementation of AES algorithm on FPGA. In Communications and Signal Processing (ICCSP), 2014 IEEE International Conference on (pp. 1895-1899).

https://rushter.com/blog/python-strings-and-memory/

https://en.wikipedia.org/wiki/Finite_field_arithmetic#Multiplication

https://www.slideshare.net/hisunilkumarr/advanced-encryption-sta