**ENCRYPTION OF IMAGE USING TRIPLE DES**

**DIPLOMA IN INFORMATION TECHNOLOGY**

**Submitted By**

##### Mrudit D. Kanjariya

**Under The Guidance Of**

###### Mr. Arvind Kumar

**R&D Engineer , Exposys Data Lab**



**Exposys Data Labs**

**Bengaluru,India**

**INDEX:**

**1. PROFILE OF THE PROBLEM**

1.1 INTRODUCTION

**2. SYSTEM STUDY**

2.1 INTRODUCTION

2.2 EXISTING SYSTEM

2.3 PROPOSED SYSTEM

**3. PROBLEM ANALYSIS**

3.1 SYSTEM DEFINITION

3.2 FEASIBILITY ANALYSIS

3.3 PROJECT PLAN

**4. REQUIRMENT ENGINEERING**

4.1 INTRODUCTION

4.2 DETAILS

**5. DESIGN**

5.1 USER INTERFACE DESIGN

5.2 CONTENT DESIGN

5.3 ARCHITECTURE DESIGN

5.4 NAVIGATION DESIGN

5.5 COMPONENT LEVEL DESIGN

**6. CODING**

6.1 INTRODUCTION

7**. THEORY**

7.1 CRYPTOGRAPHY

7.2 CRYPTOGRAPHY GOALS

**8. SOURCE CODE**

**9. CONCLUTIO**

**10. SCREEN LAYOUT**

**1. PROFILE OF THE PROBLEM**

**1.1 INTRODUCTION**

In today's world almost all digital services like internet communication, medical and military imaging systems, multimedia system needs a high-level security. There is a need for security level in order to safely store and transmit digital image containing critical information. This is because of the faster growth in multimedia technology, internet and cell phones. Therefore, there is a need for image encryption techniques in order to hide image from such attacks. In this system we use Triple DES (Data Encryption Standard) in order to hide image. Such Encryption technique helps to avoid intrusion attacks.

**2. SYSTEM STUDY**

**2.1 INTRODUCTION**

Data Encryption Standard (DES) is the block cipher which takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. It is a symmetric encryption technique which means both sender and receiver use a shared key to encrypt and decrypt the data as shown in the below Figure 1.1 The problem of this technique is that if the key is known to others the entire conversation is compromised. The 3DES block size is 64 bits and also uses a key to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt. The key basically consists of 64 bits however, only 56-bits of these are actually used by the algorithm. Eight bits are used solely for checking parity, and thereafter discarded. Hence the "effective key length is 56-bits" and it is always quoted. Every 8th bit of the selected key is discarded i.e., positions 8,16,24,32,40,48,56,64 are removed from the 64-bit key leaving behind only the 56-bit key.

**2.2 EXISTING SYSTEM**

Visual cryptography is the art and science of encryption the image in such a way that no one apart from the sender and intended recipient even realizes the original image, a form of security through obscurity. By contrast, cryptography obscures the original image, but it doesn't conceal the fact that it isn't the actual image.

## Limitations: -

The existing system doesn't provide a friendly environment to encrypt or decrypt the data(images).

The existing system supports with only one type of image format only. For example, if it is .jpeg, then it supports only that same kind of image format only.

**2.3 PROPOSED SYSTEM**

Proposed system image encryption and decryption using Triple DES algorithm provides a friendly environment to deal with image. Generally, cryptography tools support only one kind of image formats. Our application support .gif and .png formatted images and our application has been developed using swing and applet technologies, hence provides a friendly environment to users.

Problem Definition: Whenever we transmit the data(image) in the network, any unauthenticated person can read our data(image). In order to provide security to data(image) generally sender will encrypt the data(image) and send it the intended person and the receiver will decrypt the encrypted data(image) and used it. For this process we are here using Triple DES algorithm.

**3. PROBLEM ANALYSIS**

**3.1 SYSTEM DEFINITION**

In cryptography, Triple DES, officially the Triple Data Encryption Algorithm, is a symmetric-key block cipher, which applies the DES cipher algorithm three rimes to each data block.

Block size: 64 bits, Key size: 168,112 or 56 bits (keying option 1,2,3 respectively)

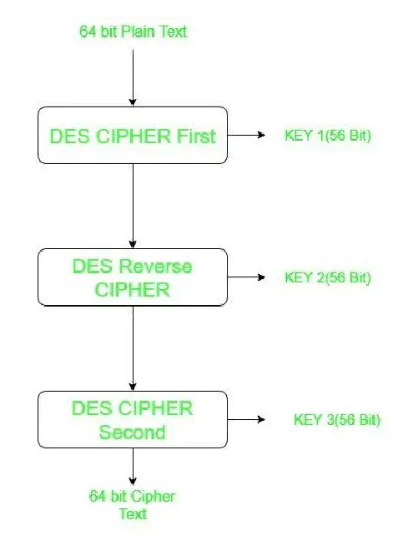
Data encryption standard (DES) uses 56 bits key to encrypt any plain text which can be easily be cracked by using modern technologies. To prevent this from happening double DES and triple DES were introduced which are much more secured than the original DES because it uses 112 and 168 bit keys respectively. They offer much more security than DES.

**Triple DES:** Triple DES is an encryption technique which uses three instances of DES on same plain text. It uses their different types of keys choosing techniques in first all used keys are different and in second two keys are same and one is different and in third all keys are same.

Triple DES encryption uses a Triple-length DATA key comprised of three 8-byte DES keys to encipher 8 bytes of data using this method:

Encipher the data using the first key Decipher the result using the second key Encipher the second result using the third key The procedure is reversed to decipher data that has been Triple-DES enciphered:

Decipher the data using the third key Encipher the result using the second key Decipher the second result using the first key.



**3.2 FEASIBILITY ANALYSIS**

A feasibility study is a test system proposal according to its workability, impact on the organization, ability to meet user needs and effective use of resources. The objective of feasibility study is acquiring of the scope of the system.

The key factors considered during the feasibility study are:

1. Economic Feasibility

2. Behavioral Feasibility

3. Technical Feasibility

4. Operational Feasibility

5. Legal Feasibility

**Economic Feasibility:**

The proposed system is economically cheaper than the previous version. This is because; almost everything in the website can be managed and controlled by the system administrator it self so they don't need the assistance of the programmer every time they wish to make any change. They don't want to buy support at a high rate. The most important fact is that, when considering the security measures of the system, the chances for risks are low and it is a great thing when talking about economy. Disaster recovery is also easily accomplished because of the design.

**Behavioral Feasibility:**

Proposed projects are beneficial only if they can be turned into information systems that will meet the Operating requirements of the organization. This test of feasibility asks if the system will work when it is developed satisfies all the operational conditions. It was the most difficult task for me, but met efficiently. As this package is found to be feasible technically, economically and functionally, the system is judged feasible. Viewing the collected information, recommendation and justification, conclusions is made of the proposed system. Hence decision is taken to go on with the project.

**Technical Feasibility:**

There are a number of technical issues, which are generally raised during the feasibility stage of the investigation. A study of function, performance and constraints gave me the ability to achieve acceptable system. The software required for this system is: MATLAB

**Operational Feasibility:**

Suppose for a moment that technical and economic resources are both judged adequate. The systems analyst must still consider the operational feasibility of the requested project. Operational feasibility is dependent on human resources available for the project and involves projecting whether the system will operate and be used once it is installed.

In this system the necessity for human resources is low because of the signal hand administration and adding shops by admin itself.

**Legal Feasibility:**

Regarding legality, our website already registered and the same domain is used here and also the certifications are updated. There no visible problem on behalf of a lawyer.

**3.3 PROJECT PLAN**

Flamming is very important in every aspect of development work. Good managers carefully monitor developments at various phase. Improper planning leads to failure of the project. Software can be viewed as the following:

1. Within the organization: How the project is to be implemented? What are various constraints? What is market strategy?

2. With respect to the customer: Weekly or timely meetings with the customers with presentations on status reports. Customer feedback is also taken and further modification and developments are done. Project milestones and deliverables are also presented to the customer.

**For a successful project the following steps can be followed:**

Selection of project: Includes identifying project's aims and objectives, understanding requirements and specification, methods of the analysis, design and implementation, testing Techniques and documentation.

1. Project milestones and deliverables.

2. Project estimates: Including cost, time, size of code and Duration

3. Resource allocation: including hardware, software, previous relevant project information and digital library.

4. Risk Manganate: including risk avoidance, risk detection, risk control and risk recovery.

5. Scheduling techniques: including work breakdown structure, activity graph, critical path method Gant chart and program, evaluation review technique.

6. People: including staff recruitment, team management and customer interaction.

7. Quality control and standard

**4. REQUIREMENT ENGINEERING**

**4.1 INTRODUCTION**

Requirement analysis involves studying the current system to find out how it works and where improvements could be made. A clear idea about the existing system is a must for making improvement where it is required. Proper planning and collection of idea of data server the purpose. The popularity of this document is to describe all the requirements for the popularity of the website Sony Cams Mark 11.

**SOFTWARE REQUIREMENTS:**

# Language: Python

Frontend: Anaconda Environment

Operating System: Windows 10

Backend: MS SQL SERVER 2012

**HARDWARE REQUIRMENTS:**

# CPU: Dual Core

Hard Disk Space: 80 GB or Above

Display: Color Monitor

Main Memory: 2 GB

Resolution: 1280x720

**4.2 DETAILS**

**PYTHON**

**Python** is an interpreted, high-level and general-purpose programming language. Python's design philosophy emphasizes code readability constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects.

Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including structured (Particularly, Procendualr), object-oriented and functional programming. Python is often described as a "batteries included" language due to its comprehensive standard library.

Python was created in the 1980s. and first released in 1991, by Guido van Rossum as a successor to the ABC programming language. Python 2.0, released in 2000, introduced new features, such as list comprehensions, and a garbage collection system with reference counting, and was discontinued with version 2.7 in 2010. Python 3.0, released in 2008, was a major with revision of the language that is not completely backward-compatible and much Python 2 code doesn't run unmodified on Python 3. With Python 2's end-of-life, only Python 3.6.x and later are supported, with older versions still supporting e.g., Windows 7 (And older installers not restricted to 64-bit Windows)

Python interpreters are supported for mainstream operating system and available for a few more (and in the past supported many more). A global community of Programmers develops and maintains CPython, a free and open-source reference implementation. A non-profit organization, the Python Software Foundation, manages and directs resource for Python and CPython development.

**Google Chrome Web Browser**

An Internet browser developed by Google Inc. that combines a minimal design with sophisticated technology to make the Web faster, safer and easier. The Google Chrome Web Browser offers features including access to favorite pages instantly with thumbnails, desktop shortcuts to launch Web application, and independently run tabs with in the browser to prevent browser crashing. Chrome browser is available for Windows and Linux.

**5. DESIGN**

**5.1 USER INTERFACE DESIGN**

User interface (UI) Design focuses on anticipating what users might need to do and ensuring that the interface has elements that are easy to access, understand, and use to facilitate those actions. UI brings together concepts from interaction design, visual design, and information architecture.

**5.2 CONTENT DESIGN**

Content Design focuses on two different design tasks, each addressed by individuals with different skill test sets. First, a design representation for content objects and the mechanisms required to establish their relationship to one another is developed. In addition, the information with in a specific content object is created. The latter task may be conducted by copywrites, graphic designers, and other who generate the content to be used with in Web-App.

**5.3 ARCHITECTURAL DESIGN**

It is tied to the goals established for a web app, the content to be presented, the user who will visit and the navigation philosophy that has been establishes. As an architecture designer, you must identify content architecture and Web-App Architecture. Content architecture focuses on the manner in which content objects are structured for presentation and navigation. Web-App Architecture addresses the manner in which the application is structured to manage user interaction, handle internet processing tasks, effect navigation and present content. Architecture design creates a blueprint for the design with the necessary specification for the hardware, software people and data resources. In this project n-Tier architecture is used foe development. It can use objects for handling business rules and data access.

**5.4 NAVIGATION DESIGN**

Once the Web-App architecture has been established and the component of the architecture has been identified, you must define navigation path way that enable users to access Web-App content and functions. To accomplish this, you should

(1) Identify the semantics of navigation for different users of the site.

(2) Define the mechanics of achieving the navigation. The main pages used in the system are, Home Page

1. Image encryption and decryption mechanism

2. Encoding

3. Decoding

**5.5 COMPONENT LEVEL DESIGN**

Modern Web-App deliver increasingly sophisticated processing function that,

(1) Perform localized processing to generate content and navigation capability in a dynamic Fashion.

(2) Provide computation or data processing capability that is appropriate for the Web-App.

Business Domains,

(3) Provide sophisticated database query and access.

(4) Establish data interface with external cooperate system.

To achieve these capabilities, we must design and construct program component that identical in from to software components for traditional software. Component level design occurs after the first interaction of architecture design has been completed. At this stage, the overall data and program structure of the software has been established. The intent is to translate the design model into operational software. The component level design represents the software in a way that allows you to review the details of the design for correctness and consistency with other design representations.

**6. CODING**

**6.1 INTRODUCTION**

The coding step is a process that transforms design into a programming language. It translates a detail design representation of software into a programming language realization. The translation process continues when a compiler code as output. Quality is an important goal during coding. The quality of source code can be improved by the use of structured coding techniques; good coding standards are to be followed. This has two purposes; reducing the chance of making it easier for some time to modify the code later on. Coding phase affects both testing and maintenance profoundly. The project uses PYTHON as the programming language for coding.

**Python** is an interpreted, high-level and general-purpose programming language. Python's design philosophy emphasizes code readability with us notable use of significant whitespace. Its language constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects.

Image encryption in cryptography segment, the restrictive or after effects of the primary bits are controlled by Associate in Nursing cryptography key utilizing a standard stream figure. It's a cryptography method that is utilized to encipher the information from unapproved people to cover the information inside the prudent way to not misfortune the information. It'll adjustment the picture into the bits on the grounds that the layers are extra made sure about from others to envision the principal picture the data should be decoded from the bits code to customary. 9.2 Data embedding in the information section, a few parameters are inserted into a little assortment of scrambled pixels are compacted to frame a region for obliging the additional data and the first information at the positions involved by the parameters. Partner degree inserting could be a relatively low-dimensional vectors. Inserting assemble it simpler to attempt to AI on mammoth information sources like slight vectors speaking to words. In a prefect world, partner degree inserting catches some of the etymology of the contribution by putting semantically comparable data sources close inside the implanting territory. 9.3 Data Extraction and Image Recovery In this part, we are going to consider the 3 cases that a beneficiary has exclusively the information concealing key, exclusively the coding key, and each the information covering up and coding keys, severally. The information and picture coding key with the help of those keys exclusively anybody can get to information and after the information asides from pictures capable to have the option to see them anyway no alterations are refreshes are feasible. In this way each the keys assumes partner significant job for data extraction.

**7. THEORY**

**7.1 CRYPTOGRAPHY**

Cryptography means data secure, it helps to ensure data privacy, maintain data integrity, authenticate communicating parties and prevent repudiation.

**7.2 CRYPTOGRAPHY GOALS**

This section explains the five main goals behind using Cryptography. Every security must provide a bundle of security functions that can assure the secrecy of the system.

* Authentication: Authentication means before sending and receiving data using the system, the receiver and sender identify should be verified.
* Secrecy or Confidentiality: In these functions is how most people identify a secure system. It means only the authenticated people are able to interpret the message or content and no one else.
* Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end point (Sender and Receiver). The basic from of integrity is packet check sum in IPv4 packets.
* Non-Repudiation: In this function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.
* Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users.

**ADVANTAGES OF DES ALGORITHM:**

1. DES has been around a long time (Since 1977), even no real weaknesses have been found: the most efficient attack is still brute force.
2. DES is an official United States Government standard; the Government is required to re-certify, DES every five years and ask it be replaced if necessary. DES has been recertified in 1983, 1987, 1992.
3. DES is also an ANSI and ISO standard. Since DES was designed to run on 1977 hardware, it is fast in hardware and relatively fast in software.

**DISADVANTAGES OF DES ALGOTITHEM:**

1. The 56-bit key size is the biggest defect of DES and the chips to perform one million of DES encrypt or decrypt operation a second are available (in 1993).
2. Hardware implementation of DES are very fast.
3. DES wasn't designed for software and hence runs relatively slowly.
4. In a new technology it is improving a lot of possibility to break the encrypted code, so AES is preferred than DES.

**8. SOURCE CODE**

from Crypto.Cipher import DES3

from Crypto.Random import get\_random\_bytes

from PIL import Image

import io

# Function to pad the data to be a multiple of the block size (8 bytes for DES)

def pad(data):

    while len(data) % 8 != 0:

        data += b' '

    return data

# Function to encrypt the image

def encrypt\_image(image\_path, key):

    # Open the image and convert it to bytes

    with Image.open(image\_path) as img:

        img\_byte\_array = io.BytesIO()

        img.save(img\_byte\_array, format=img.format)

        img\_bytes = img\_byte\_array.getvalue()

    # Pad the image bytes

    padded data = pad(img\_bytes)

    # Create a Triple DES cipher object and encrypt the data

    cipher = DES3.new(key, DES3.MODE\_ECB)

    encrypted\_data = cipher.encrypt(padded\_data)

    return encrypted\_data

# Function to decrypt the image

def decrypt\_image(encrypted\_data, key, output\_path, format):

    # Create a Triple DES cipher object and decrypt the data

    cipher = DES3.new(key, DES3.MODE\_ECB)

    decrypted\_data = cipher.decrypt(encrypted\_data).rstrip(b' ')

    # Convert bytes back to an image and save it

    image = Image.open(io.BytesIO(decrypted\_data))

    image.save(output\_path, format=format)

# Example usage

key = get\_random\_bytes(24)  # 24 bytes for Triple DES (3 \* 8 bytes)

encrypted\_image = encrypt\_image('input\_image.jpg', key)

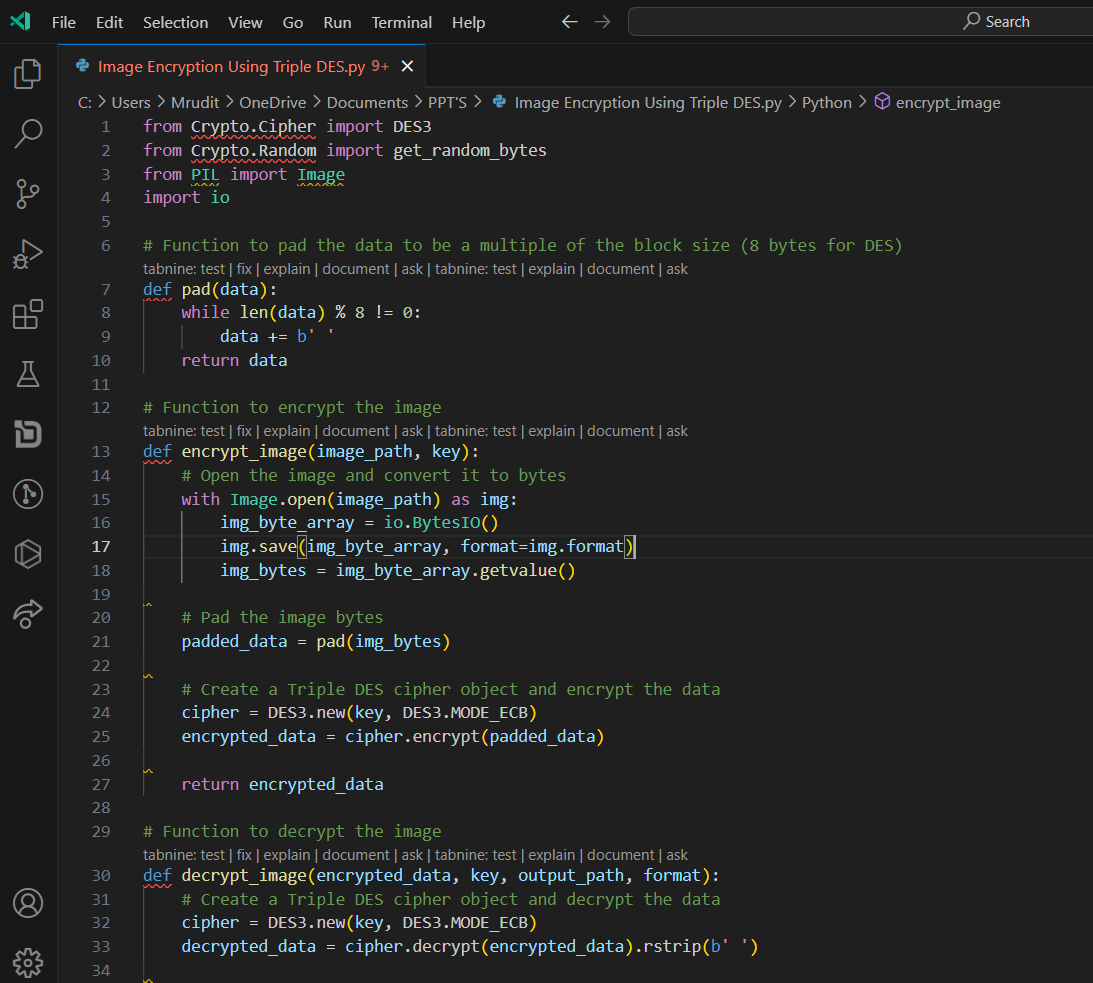
decrypt\_image(encrypted\_image, key, 'output\_image.jpg', 'JPEG')

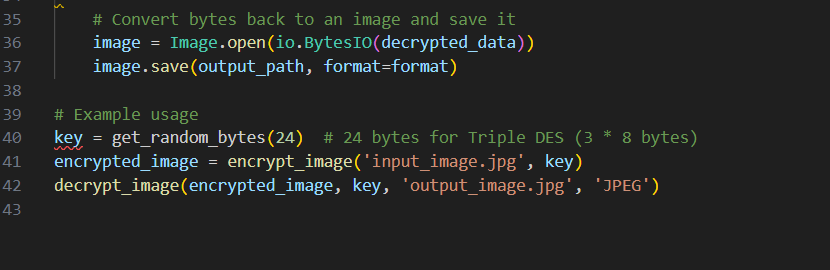
**9. CONCLUSION**

The presented simulation result showed that 3DES has a better performance result with ECB and CBC than other common encryption algorithms used. In this paper we present a performance evaluation of selected symmetric encryption algorithms. In case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption. In future the work may be extensive by including the schemes and techniques over different types of data such as image, Sound and video rising a stronger encryption algorithm.

This algorithm uniquely defines the mathematical steps required to transform the image into a cryptographic cipher and also to transforms the cipher image back to its original form. Therefore, it also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.

**10. SCREEN LAYOUT**

****

****

**I can't able to make a Crypto.cipher And Crypto.Ramdom Module.Because I can't understand a how to make a cryptography module like mention.**