`

Annexure 1

Project Report
on

AES-based encryption in a GUI application

Submitted

In Partial Fulfillment of

BACHELOR OF COMPUTER APPLICATIONS (BCA)

Submitted by:

1.

Name – Ashish Kargeti
(Roll No)- 23/SCA/BCA(DS&BDA)/006

Under the Supervision of: Ms .Aastha Budhiraja

(Data confidentiality via AES-based encryption in a GUI application)

School of Computer Applications
Manav Rachna International Institute of Research and Studies
(DEEMED TO BE UNIVERSITY)
Sector-43, Aravalli Hills
Faridabad – 121001

June 2025

`

Annexure 2

Declaration

I do hereby declare that this project work entitled "Data confidentiality via AES-based encryption in a GUI application" submitted by me for the partial fulfillment of the requirement for the award of **BACHELOR OF COMPUTER APPLICATIONS** is a record of my own work. The report embodies the finding based on my study and observation and has not been submitted earlier for the award of any degree or diploma to any Institute or University.

Name:

Ashish Kargeti

Roll

No: 23/SCA/BCA(DS&BDA)/006

Date:

15th July 2025

`

Certificate from the Guide

This is to certify that the project report entitled **"AES-based encryption in a GUI Application "** submitted in partial fulfillment of the degree of **Bachelors OF COMPUTER APPLICATIONS** to   Data Confidentiality via AES-based Encryption in a GUI Application

This project is a Python-based GUI application designed to demonstrate the use of AES (Advanced Encryption Standard) for message encryption and decryption. Built using Tkinter for the interface and PyCryptodome for cryptographic functions, it ensures a secure and user-friendly way to handle sensitive data.

The application allows users to input a message and a secret key, and based on their selection (Encrypt or Decrypt), it performs the respective AES operation. The system uses Base64 encoding and appropriate padding to maintain compatibility with AES encryption standards.

The project was developed as part of a 4-week internship in the Cybersecurity Department at GKN Automotive, where I worked on applying core encryption techniques in a practical environment. This experience helped me understand the relevance of data confidentiality in real-world scenarios and how even simple tools can enhance information security.

Manav Rachna International Institute of Research and Studies, Faridabad is carried out by **Mr. Ashish Kargeti** (Roll No), **23/SCA/BCA(DS&BDA)/006** under my guidance.

Signature of the Guide

Name: **Aastha Budhiraja**

Date: **15th july 2025**

Head of Department

Name : Dr. Suhail Javed Quraishi

Date   : 15th July 2025

`

ACKNOWLEDGEMENT

I gratefully acknowledge for the assistance, cooperation, guidance and clarification provided by **Ms. Aastha Budhiraja** during the development of the **project titled "Data Confidentiality via AES-based Encryption in a GUI Application** My extreme gratitude to **Dr. Raj Kumar, Associate Professor & TPO** who guided us throughout the project. Without his willing disposition, spirit accommodation, frankness, timely clarification and above all faith in us, this project could not have been completed in due time. His readiness to discuss all important matters at work deserves special attention of.

I would like to extend my sincere gratitude to **Prof. (Dr.) Suhail Javed Quraishi – HOD, Prof. (Dr.) Rashmi Agrawal – Associate Dean and Prof. (Dr.) Brijesh Kumar – Dean** for their valuable teachings and advice. I want to thank all the department faculty members for their cooperation and support. I want to thank non-teaching staff of the department for their cooperation and support.

This opportunity is a big milestone in my career development. I will strive to use gained skills and knowledge in the best possible way, and I will continue to work on their improvement, to attain desired career objectives. I hope to continue cooperation with all of you in the future.

`

ABOUT THE ORGANIZATION

✶ GKN AUTOMOTIVE – PIONEERING INNOVATION AND MOBILITY

GKN Automotive is a global powerhouse in the automotive industry, renowned for engineering excellence, innovation, and a rich legacy spanning over **250 years**. With its headquarters in the United Kingdom, the company operates across **20+ countries**, delivering state-of-the-art driveline technologies and ePowertrain systems to more than **90% of global car manufacturers**.

As a **world leader in automotive drive systems**, GKN Automotive plays a pivotal role in shaping the future of mobility. The company is at the forefront of the electric revolution, driving transformation with its cutting-edge **electric vehicle (EV) technologies**, intelligent control systems, and lightweight, sustainable engineering solutions.

In addition to mechanical excellence, **cybersecurity** has emerged as a crucial domain for the company. With vehicles becoming smarter and more connected, GKN Automotive is investing in securing its digital ecosystems, protecting sensitive data, and ensuring that vehicle control systems remain uncompromised. Their cybersecurity departments focus on encryption, secure communication protocols, and robust digital defense frameworks that align with international standards.

With a workforce of over **25,000 skilled professionals**, GKN Automotive cultivates a culture of **technical mastery**, **collaboration**, and **sustainability**. The company is committed to advancing not just the performance of automobiles, but also the digital backbone that supports their safety and reliability.

The opportunity to intern at such a globally respected organization has provided me with firsthand exposure to the real-world challenges and solutions in the field of **data confidentiality and encryption**—skills that are vital in today's data-driven, technology-centric era.

For more information, you may visit their official LinkedIn profile:
GKN Automotive on LinkedIn

`

AIMS AND OBJECTIVES

Project Focus: Securing Data Through Encryption

The primary aim of this project is to develop a practical and secure **AES-based encryption and decryption system** with an intuitive graphical user interface (GUI), providing confidentiality and control to users over their digital information.

In today's digital age, where cyber threats are constantly evolving, the need to **safeguard sensitive data** is more important than ever. Through this project, I have aimed to contribute toward this goal by building a system that incorporates advanced encryption techniques in a **user-friendly, real-time application**.

✅ Key Objectives of the Project

To study and implement the **Advanced Encryption Standard (AES)** – a widely trusted and secure symmetric key encryption algorithm.

To design a **GUI-based application** using Python and Tkinter that allows users to encrypt and decrypt custom messages or strings.

To provide an intuitive and reliable user interface that ensures data confidentiality without needing deep technical knowledge.

To simulate **real-world cybersecurity applications** by combining theoretical knowledge with hands-on practical implementation.

To increase awareness of **data protection mechanisms** and demonstrate how simple tools can enhance personal and organizational data security.

To understand **cryptographic workflows** and learn how encryption can be integrated into modern software systems.

`

PROPOSED SYSTEM SUMMARY

⬣ An AES-Integrated GUI Application for Data Confidentiality

The proposed system is a **Python-based GUI application** that implements the **Advanced Encryption Standard (AES)** to ensure the confidentiality of digital messages. Built with simplicity and efficiency in mind, this application empowers users to securely **encrypt** and **decrypt** sensitive information without requiring in-depth knowledge of cryptographic algorithms.

In an era where data is one of the most valuable assets, ensuring its security is not just important—it is essential. This system is designed to address that need by offering an easy-to-use yet highly secure platform that facilitates the encoding and decoding of text-based messages.

Developed using **Tkinter for the graphical interface** and **PyCryptodome for encryption**, the application follows a structured flow. The user is prompted to input a secret key and a message. Based on the user's choice, the system then processes the input through the AES algorithm—either encrypting it into an unreadable ciphertext or decrypting it back into plain text. The system ensures proper padding, block size compliance, and Base64 encoding for a seamless and accurate cryptographic operation.

⚙ Key Features of the Proposed System

   User-Friendly Interface: Clean and interactive design using Tkinter, allowing smooth navigation for both encryption and decryption tasks.
   Secure AES Implementation: 128-bit AES encryption standard ensures high-level data protection.
   Symmetric Key Usage: The same key is used for both encryption and decryption, keeping the process straightforward yet secure.
   Modular Design: The code is structured in functions that make it readable, maintainable, and reusable.
   Real-Time Results: Immediate output display of encrypted or decrypted text on the GUI.
   Compact and Lightweight: The program does not require heavy resources and is easy to deploy.

This system is especially useful for individuals or organizations who handle sensitive data and want a quick way to protect their information. The combination of **cryptographic strength** and **ease of use** makes this system a practical solution for enhancing data privacy in day-to-day operations

`

📊 GANTT CHART

📑 Project Timeline and Task Allocation (4-Week Duration)

The following Gantt Chart outlines the week-wise progress plan for the completion of the project titled
"Data Confidentiality via AES-based Encryption in a GUI Application."

This breakdown provides a clear visualization of how the tasks were managed and executed during the vocational training period.
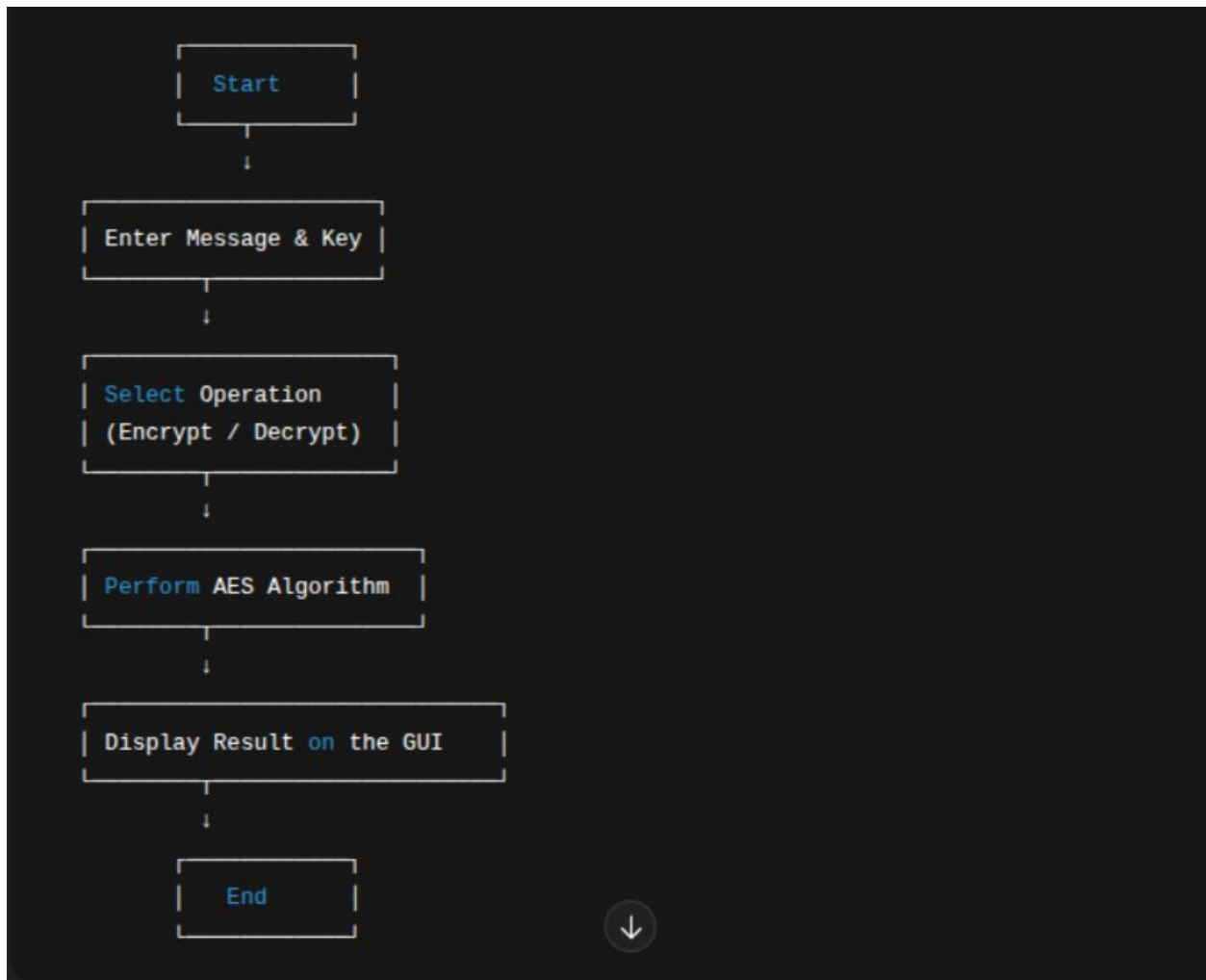
Week	Task Description	Duration	Status
Week 1	🔍 Requirement Gathering & System Analysis	16th June – 20th June	✅ Completed
Week 2	🛠 System Design & GUI Wireframing	21st June – 25th June	✅ Completed
Week 3	🖥 Implementation (AES Logic + GUI Integration)	26th June – 2nd July	✅ Completed
Week 4	Testing, Debugging, Report Writing & Submission	3rd July – 11th July	In Progress / Done

`

DFD / FLOWCHART

Understanding the Functional Flow of the System

To better visualize the internal operations of the AES-based encryption application, this section presents both a **Data Flow Diagram (DFD)** and a **System Flowchart**. These visual models provide insight into how user data is processed within the system, from input to output.

⌁ Level 1 Data Flow Diagram (DFD)

Key Components:

- **User Interface (GUI):** Facilitates data entry and displays results.
- **AES Core Logic:** Handles secure encryption and decryption using a symmetric key.

`

- **Controller Module:** Routes the user's action to the correct cryptographic function.
GITHUB LINK **(Ashish Kargeti)** https://github.com/ashishkargeti