CONFIGURATION MANUAL

MSc Internship

MSC IN CYBERSECURITY

SHUBHAM

Student ID: X21177163

School of Computing

National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……..…… SHUBHAM……

Student ID: ……X21177163……..……

Programme: ……. MSC IN CYBERSECURITY …… **Year:** …2023…

Module: …… ACADEMIC INTERNSHIP ……..……

Supervisor: …… Niall Heffernan ……..……

Submission Due Date: ……14-08-2023……..……

Project Title: CONFIGURATION MANUAL

Word Count: **969** **Page Count: 9**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……Shubham……

Date: ……14—8-2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

CONFIGURATION MANAUAL

Contents

1. Introduction

This research presents an approach to enhance data encryption effectiveness and security through the use of a combination of techniques. The main objectives of the project are as follows:

- In this method, a hybrid approach is developed by combining AES encryption for the original text and ECC keys to re-encrypt the cipher text after retrieval. By adding an extra layer of security, this approach becomes particularly useful in situations where prioritizing security is more important than efficiency.
- Another technique employed in this project involves encrypting the original text message using a new AES key after the old AES key has been encrypted using ECC. The efficiency is improved because the encryption is done on the key itself rather than the plain text communication. This method is preferable when effectiveness is more crucial than data storage concerns.
- The research also utilizes a hybrid technique where the AES key is split into four parts, and one of those pieces is encrypted using the ECC algorithm. This process generates a new AES key, which is then used to encrypt the plain text. This approach reduces the encryption time and enhances security, as cybercriminals would need to decrypt the key before attempting to decrypt the encrypted content. This additional layer of security ensures efficiency while maintaining strong protection.

By implementing these innovative methods, the research aims to create a robust encryption algorithm that can be adapted to different scenarios based on the specific requirements of security and efficiency.

2. System Configuration

The Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) are combined in the provided code to create a hybrid method that increases the security of data encryption and decryption operations. There are particular sorts of equipment and resources needed to efficiently run this algorithm. A computer or other computing device that can run MATLAB or a similar programming environment is first and foremost required. Additionally, the device must have a trustworthy and secure storage medium in order to guarantee the security of the encrypted data. Overall, the hybrid method can offer a reliable and secure data encryption solution for a variety of applications because its performance is dependent on the device's processing power, memory, and storage capacity.

2.1 Hardware Configuration

A device with enough Random Access Memory (RAM) is advised to handle the processing of huge data sets successfully because the method uses memory resources. AES and ECC implementation software libraries, functions, and scripts may need to be downloaded and stored, which will add to the algorithm's potential storage space requirement. For both AES and ECC, sufficient computer capacity is required to carry out the intricate mathematical processes. The encryption and decryption procedures can be substantially sped up by a modern CPU with multiple cores.

2.2 Software Configuration

MATLAB: We choose MATLAB for our research after completing in-depth research on a number of testing environments for encryption techniques. This choice is being supported by a number of factors. First off, MATLAB is an effective software suite that offers a variety of tools and functions for testing and assessing encryption schemes. It is perfect for academics and developers with varied degrees of programming knowledge because it also has a user-friendly interface and simple syntax. A large number of encryption-related functions and toolboxes have also been developed by the MATLAB community, which has helped to save a lot of time and effort during the testing stage.

Requirement:

Operating System	• Windows 11 • Windows 10 (version 1909 or higher) • Windows Server 2019 **Note:** • Windows 7 is no longer supported • Windows Server 2016 is no longer supported
Processor	• Minimum: Any Intel or AMD x86-64 processor • Recommended: Any Intel or AMD x86-64 processor with four logical cores and AVX2 instruction set support
RAM	• Minimum: 4 GB • Recommended: 8 GB • For Polyspace, 4 GB per core is recommended
Storage	• 3.6 GB for just MATLAB • 5-8 GB for a typical installation • 31.5 GB for an all products installation • An SSD is strongly recommended
Graphics	• No specific graphics card is required, but a hardware accelerated graphics card supporting OpenGL 3.3 with 1GB GPU memory is recommended. • GPU acceleration using Parallel Computing Toolbox requires a GPU that has a compute capability 3.0 or higher. For more information, see GPU Support by Release.

Cryptool2: A range of cryptographic algorithms and techniques for encryption, decryption, and protocol analysis are available in the free and open-source cryptography application Cryptool 2.

Requirement:

Cryptool2 is an open-source software which is available for windows, Linux and macOS.

AIDA64:

Requirements:

You will need a computer running a compatible operating system, such as Windows or Linux, in order to install AIDA64 Extreme, a thorough system diagnostics and benchmarking program.

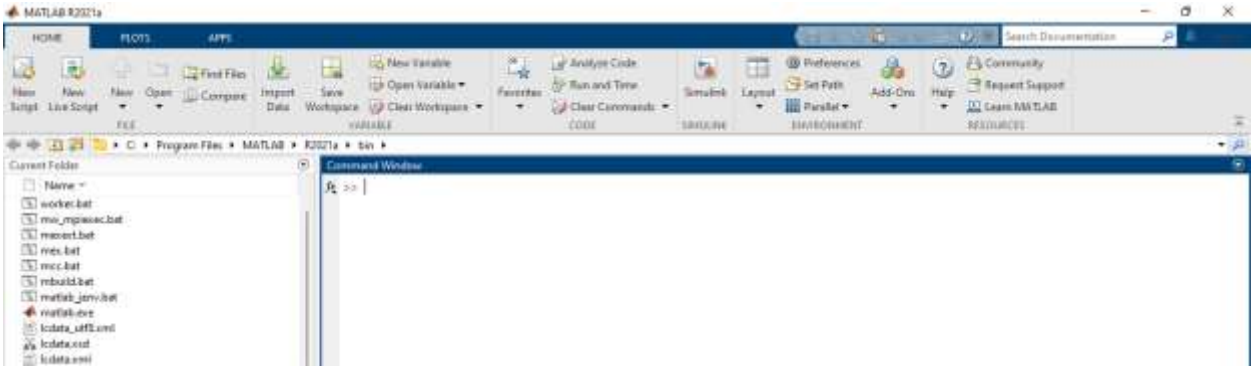
3. Steps to Run the Code:

A sequence of actions must be taken in order to start the code's execution and explore its functionality. These actions cover the preparation and setting up needed for a smooth code run. Following these guidelines will help consumers have a seamless and successful experience.

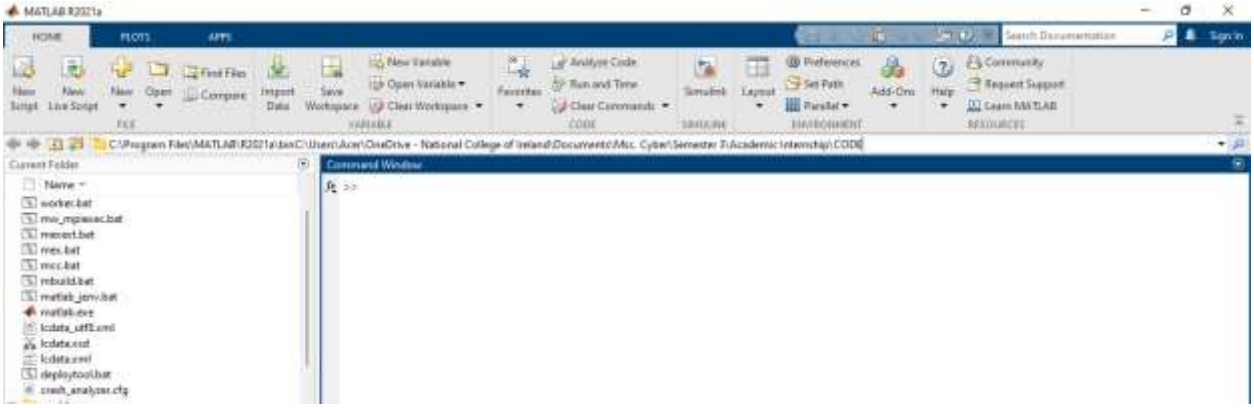
Step1: Install the MATLAB software from the website ‘www.mathswork.com’.

Step2: Download the code zip file and extract the ‘CODE’ folder.

Step3: Open the installed MATLAB Software.



Step4: Now, click on browse or open folder button or paste the path of folder in the bar and click ‘Enter’.



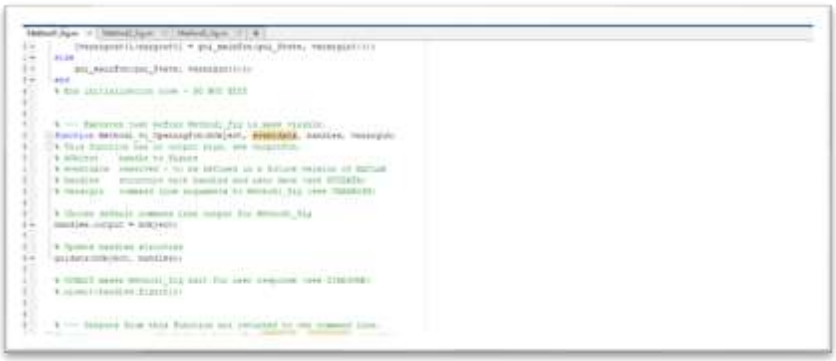
Step5: Now Run the Method1_fig.m, Method2_fig.m, Method3_fig.m file.

4. IMPLEMENTATION

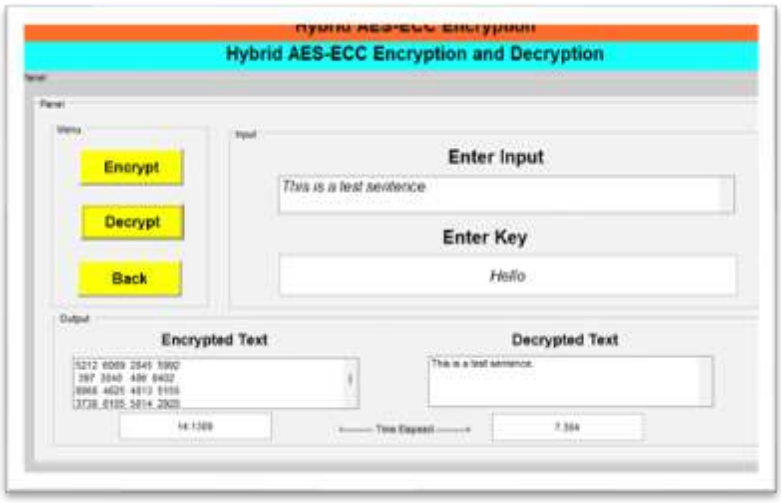
METHOD 1:

With the help of both keys, this method encrypts the plain text by first using AES and then using ECC to encrypt the cipher text that is produced. This is the most straightforward technique of encryption.

CODE:



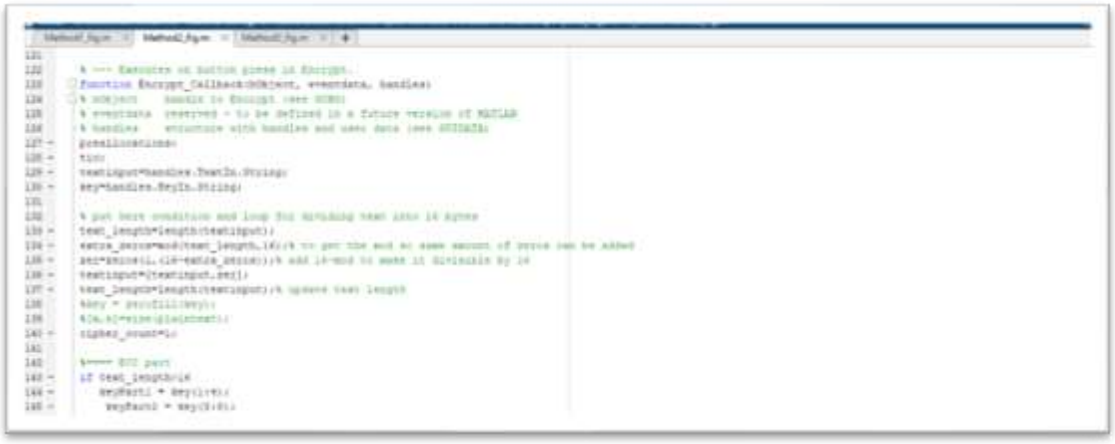
OUTPUT:



Method 2:

In the Method 2, enter the key of 16 bytes because in this method key is divided into 4 parts and 4th part of the key is encrypted.

CODE:

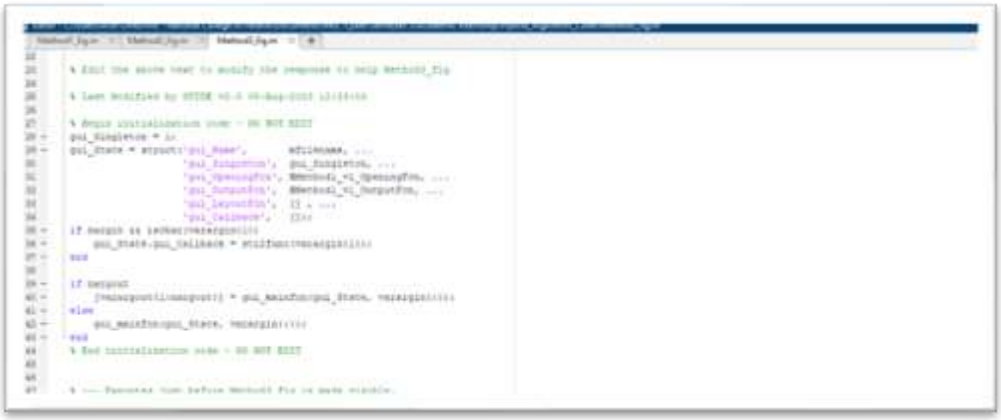


Output:

Method 3:

In this method, the AES key is encrypted first using ECC and then the new AES key is used to encrypt the plaint text.

CODE:



OUTPUT:

5. Conclusion

The researcher investigated the impact of utilizing a combination of two encryption algorithms, namely symmetric and asymmetric encryption. This study involved the fusion of AES and ECC encryption methods in various manners, some of which demonstrated superior outcomes compared to others. Initially, the first approach yielded commendable security and randomness characteristics; however, this was offset by prolonged execution times. Subsequently, the second approach led to enhanced execution times while marginally compromising on randomness compared to the first method. Lastly, the third approach offered equivalent execution times to the second method and comparable randomness to the first method. Consequently, the researcher recommended the adoption of hybrid encryption. When implemented effectively, this approach has the potential to harness the advantages of each method while mitigating their respective drawbacks.