APPROACH FOR INCREASING EFFECTIVENESS OF ENCRYPTION FOR SECURING DATA

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: APPROACH FOR INCREASING EFFECTIVENESS OF ENCRYPTION FOR SECURING DATA

Word Count: **5227** **Page Count: 20**

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):	

Approach for Increasing Effectiveness of Encryption for Securing Data

SHUBHAM

21177163

Masters in Cybersecurity

National College of Ireland

ABSTRACT

With the increasing reliance on digital data transfer, strong encryption is now essential to protect data from unauthorized access. Hybrid encryption, which blends the advantages of many encryption methods, is one practical method for enhancing data security (Agarwal et al., 2021). In order to strengthen data security, this study offers an innovative approach which utilizes the Advanced Encryption Standard (AES) with the use of ECC encryption techniques.

The suggested approach makes use of the special benefits of both the AES and ECC algorithms. AES is a well-known symmetric encryption technique that can handle enormous volumes of data thanks to its quick encryption and decryption speeds. ECC, on the other hand, is a public-key encryption method that uses lower key sizes and delivers improved security when compared to more conventional techniques like RSA.

Simulations were run and compared to other encryption strategies to determine how effective the proposed hybrid encryption approach was. The outcomes show that the proposed strategy accomplishes a high standard of security while maintaining computational efficiency. This result implies that the suggested approach has been promised as a practical choice for protecting confidential information in the digital sphere.

Keywords: Encryption, AES, ECC, Research, Key.

Contents

1. Introduction 6

1.1 Research Question: 6

1.2 Goal and Purpose: 6

2. Literature Review 7

2.1 Introduction 7

2.2 Related Work 8

2.3 Research Gap: 10

3. Research Methods 11

3.1 Introduction 11

3.2 Primary and Secondary Sources 11

3.3 Quantitative Research 11

3.4 Procedural approach 11

3.5 Software Used 12

3.6 Metrics 13

3.7 Analysis 14

4. Design and Implementation 14

4.1 Method 1 14

4.2 Method 2 15

4.3 Method 3 17

4.4 Code Analysis: 18

5. Results and Discussion 18

6. Conclusion and Future Work 22

7. References 23

Table of Figures:

Figure 1 AES Encryption process scheme 7
Figure 2 Point Addition of Elliptic Curve Figure 3 Point Multiplication of Elliptic Curve 8
Figure 4 List of researched papers, their findings, and limitations 10
Figure 5 Research Gap 10
Figure 6 Procedural approach for Methods 11
Figure 7 List of tools and their function 13
Figure 8 Encryption Process of Method 1 14
Figure 9 Decryption process of Method 1 15
Figure 10 Encryption process of Method 2 15
Figure 11 Decryption process for Method 2 16
Figure 12 Encryption process for Method 3 17
Figure 13 Decryption process for Method 3 17
Figure 14 Profiler Tool in MATLAB 18
Figure 15 Comparing time taken for Encryption and Decryption by different algorithms. 19
Figure 16 Comparing CPU Clock for Encryption and Decryption by different algorithms. 19
Figure 17 Profiler tool showing time execution of different command lines 20
Figure 18 Encryption of plain text with key '01010101' 21
Figure 19 Encryption of plaintext with key '01010100' 21

1. Introduction

Today's digital environment has made data a valuable asset, thus protecting its security is important. Cyber risks have increased as a result of people's increasing reliance on the internet(Rehman et al., 2021). Data protection during transfer is a crucial component of overall information security since cybercriminals might intercept and exploit data carried over the internet.

The hybrid encryption strategy used in this study, which combines the potent algorithms AES and ECC, provides a revolutionary method for improving the effectiveness of data encryption. The suggested technique gives a number of benefits by combining the best features of AES and ECC. Fast encryption and decryption are made possible by the widely used symmetric encryption algorithm AES, making it perfect for processing massive amounts of data. However, compared to conventional RSA, the public-key encryption technique ECC offers strong security with the added advantage of reduced key sizes.

The study intends to strengthen data security during transmission and successfully fend off potential cyber-attacks through the integration of AES and ECC in this hybrid encryption approach.

1.1 Research Question:

R.Q. How much does a hybrid encryption method that combines the AES and ECC algorithms improve on other encryption techniques in terms of data security?

The main objective of this study is to determine whether the AES and ECC hybrid encryption method is more efficient than other hybrid encryption algorithms, such as AES+RSA, AES+SHA, AES+ElGamma, etc., in terms of speed and security. The study's objective is to compare the findings of this investigation with those of previous investigations into various hybrid algorithms in order to determine which hybrid technique is optimal for data encryption and decryption.

1.2 Goal and Purpose:

The objective of this project is to create an algorithm using a combination that improves the operation's reliability and security by doing the following:

- A hybrid technique is created, combining AES to encrypt the original text and ECC keys to re-encrypt the cipher text after it has been retrieved. This provides an additional layer of security for the information and may be utilized in situations when security takes precedence above efficiency.
- We employ yet another hybrid technique in which the AES key is divided into four pieces and one of those pieces is encrypted using the ECC algorithm, resulting in the creation of a new AES key that will be applied for the encrypting of the plain text. This technique shortens the encryption process and improves security because the cybercriminal must first decrypt the key before they can decrypt the encrypted content. The approach becomes more efficient by adding a second layer of security while requiring less time for encryption.

- Another method is employed in this project, where the original text message is encrypted using the new AES key after the old AES key has been encrypted using ECC. The efficiency of this method is increased because the key itself is encrypted rather than the plain text communication. When effectiveness is of greater significance than data, this strategy may be applied.

The reason to choose AES is that it is the most effective way for encrypting huge amounts of data, while ECC was chosen because ECC provide same level of security as other asymmetric algorithm but with smaller key sizes which increases its performance.

2. Literature Review

2.1 Introduction

According to the study of (Hercigonja, 2016), cryptography is essential for securely encrypting and decrypting data. The article describes how cryptography is made using computational methods and keys, which are essential components in the data modifying process. The study highlights the crucial security properties of cryptography, such as confidentiality, data integrity, and authentication, all of which are made possible by the employment of encryption and decryption techniques. This work provides a comprehensive understanding of the essential ideas of cryptography for any research in the field of data security. The primary goal of encryption, according to the paper by (Nadeem and Javed, 2005), is to ensure the secrecy and integrity of data. However, the performance impact of encryption techniques must also be taken into account. Ineffective encryption methods can seriously impede data processing and transmission, which is troublesome for applications with high traffic volumes like e-commerce, banking, games, etc. Performance is consequently crucial for encryption.

A well-liked technique for protecting data transmission over the internet is encryption. Ordinary text is converted by encryption techniques into cipher text, which is unreadable by unauthorized parties. The encryption text is converted back to plain text for authorized users using decryption techniques. Asymmetric, symmetric, and hashing encryption techniques are only a few of the options.

Symmetric encryption, in which the same key is used for both encryption and decryption. The Advanced Encryption Standard (AES) is the favored symmetric encryption algorithm(Mouha). Massive volumes of data may be quickly encrypted and decrypted using a block-cipher technology called AES. The fundamental disadvantage of symmetric encryption is that both the sender and recipient must securely exchange the key.

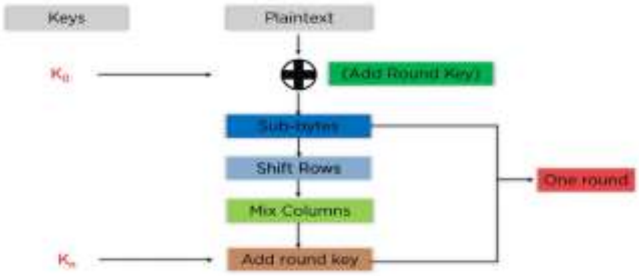


Figure 1 AES Encryption process scheme

- **Asymmetric encryption**, uses many keys for encryption and decoding, commonly known as public-key encryption. Elliptic Curve Cryptography (ECC) is a cutting-edge encryption method that uses the elliptic curve's mathematical features over finite fields to ensure secure data transmission(Journal). The basic equation for the curve is 2 = 3 + + y 2 =x 3 +ax+b, where a and b are constants defining the curve and x and y are the coordinates of points on the curve.

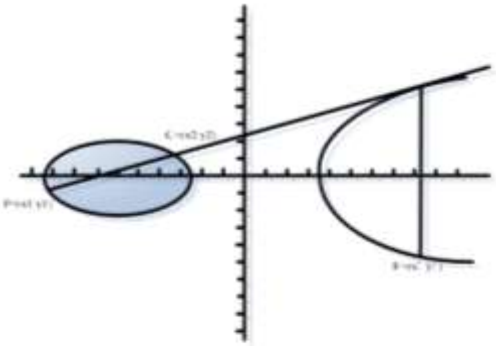


Figure 2 Point Addition of Elliptic Curve

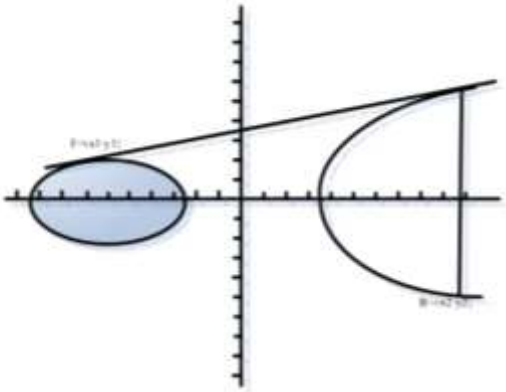


Figure 3 Point Multiplication of Elliptic Curve

- **Hashing** is a method for turning any amount of data into a fixed amount of output known as a hash value. For message integrity checks and authentication, hashing is employed. On the other hand, hashing is a one-way process that cannot be decrypted.

Even though several encryptions have advantages, none of them can be considered complete secure. Experts have therefore created hybrid encryption, which combines the benefits of two or more encryption techniques. Hybrid encryption produces a more robust and secure encryption solution by fusing the advantages of different encryption techniques.

The importance of encryption has been researched for decades and is now more important than ever due to the expansion of internet usage and the digitization of communication. The benefits and drawbacks of different encryption techniques and algorithms are well known to experts in cryptography. No one encryption technique, according to (Al Mamun et al., 2021),can guarantee the best level of security and efficacy in every application scenario. They created hybrid encryption, a system that combines the benefits of numerous encryption algorithms, in order to improve security and performance. To improve the security and efficiency of digital communication, experts in the field of cryptography have created hybrid encryption, demonstrating their expertise, know-how, and commitment in the process.

2.2 Related Work

Several academics suggested combining several techniques to boost security and effectiveness.

The study by (Li et al., 2010) makes a contribution to the field of encryption algorithms by outlining an innovative method that combines an enhanced version of the AES (Advanced Encryption Standard) with the ECC (Elliptic Curve Cryptography) encryption. The suggested hybrid algorithm takes into account many aspects of data transport and security. It not only speeds up the encryption and decryption procedures but also addresses the tricky key distribution problem. The algorithm also has authentication capabilities, which are highlighted by its quick computation time and resistance to attacks. The research aims to greatly improve the security of data transmission operations by integrating these aspects. This ground-breaking contribution improves on currently used encryption methods and provides a thorough response to the complex problems posed by data security and transmission.

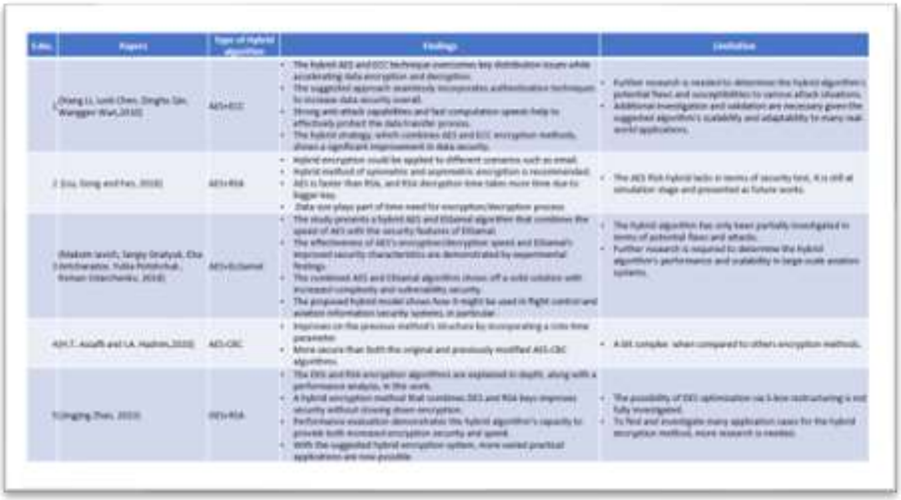
AES and RSA are used in combination in the study by (Liu et al., 2018) to develop a hybrid encryption technique for email communication. The authors highlight the adaptability of these algorithms and describe how to apply them in practical situations. The report claims that RSA encryption is better suited to authentication situations, whereas AES encryption is faster and better suited to encrypting large volumes of data. The authors also claim that because there are fewer keys to manage with RSA, key distribution is easier. The authors suggest a technique for secure key distribution that uses RSA to encrypt the AES keys while using AES to encrypt messages. The study emphasizes the necessity of email communication speed and points out that the encryption and decryption processes.

The study by (Iavich et al., 2018) explores cryptographic systems with a particular emphasis on the differences between symmetric and asymmetric cryptosystems. The work presents a hybrid method that combines the AES and ElGamal cryptosystems, which brings a fresh approach. The creation and implementation of a customized software tool especially designed for the suggested hybrid system go hand in hand with this notion. The report uses actual research to compare the encryption and decryption speeds, identifying AES as an effective symmetric choice and ElGamal as an asymmetric alternative that prioritizes security. AES is particularly noted for its high level of computational efficiency and prestigious place in symmetric encryption cryptography. ElGamal, in contrast, has a high throughput compared to AES and other algorithms. The combination of AES and ElGamal confers a special strength, giving the hybrid algorithm a blend of their own traits and boosting its resistance to weaknesses. By beating ElGamal in encryption/decryption speed and outperforming AES in terms of security, the resulting hybrid model proves to be a strong substitute. This hybrid solution, which carefully balances the two algorithms, has a lot of potential for use in the aviation industry, especially for improving the security of vital aviation information systems and flight control systems.

In order to improve security, (Assafli and Hashim, 2020) present a new modified AES-CBC encryption scheme. The structure of the proposed approach is improved by the addition of a Unix time parameter. The effectiveness of the altered AES-CBC was evaluated according to the Avalanche Effect criteria. The study's conclusions show that the improved AES-CBC technique is more secure than both the original and earlier improved AES-CBC methods. Since it presents a cutting-edge technique for enhancing the security of the AES-CBC algorithm, this makes a substantial addition to the field of encryption. The findings of this study may be helpful to people and organizations looking for solutions to secure sensitive data and information.

The study by (Zhao, 2023) provide a thorough and in-depth explanation of two important encryption algorithms: the symmetric DES and the asymmetric RSA. The report emphasizes that while DES provides faster encryption, security issues are raised by its shorter key length and secret S-box core. However, RSA uses longer keys at the expense of decreased efficiency in order to increase security.

In recognition of these advantages and disadvantages, the study suggests a novel strategy—a hybrid encryption system integrating DES and RSA. In this method, the DES key is encrypted using RSA before it is used to encrypt the plaintext. The study emphasizes the hybrid algorithm's potential to retain encryption speed while providing increased security through performance analysis, suggesting wider practical applications.

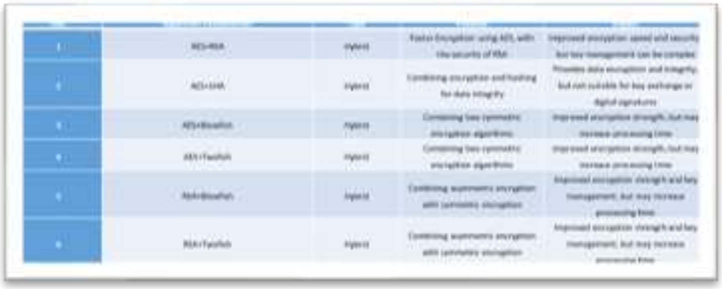


S.No.	Papers	Type of hybrid algorithm	Findings	Limitation
1	(Qiang Li, Lunli Chen, Dingfei Qin, Wanggen Wan, 2018)	AES+ECC	• The hybrid AES and ECC technique overcomes key distribution issues while accelerating data encryption and decryption. • The suggested approach seamlessly incorporates authentication techniques to increase data security overall. • Strong anti-attack capabilities and fast computation speeds help to effectively protect the data transfer process. • The hybrid strategy, which combines AES and ECC encryption methods, shows a significant improvement in data security.	• Further research is needed to determine the hybrid algorithm's potential flaws and susceptibilities to various attack situations. • Additional investigation and validation are necessary given the suggested algorithm's scalability and adaptability to many real-world applications.
2	(Liu, Song and Fan, 2018)	AES+RSA	• Hybrid encryption could be applied to different scenarios such as email. • Hybrid method of symmetric and asymmetric encryption is recommended. • AES is faster than RSA, and RSA decryption time takes more time due to bigger key. • Data size plays part of time need for encryption/decryption process	• The AES RSA hybrid lacks in terms of security test, it is still at simulation stage and presented as future works.
3	(Maksim Iavich, Sergiy Gnatyuk, Elza Jintcharadze, Yuliia Polishchuk, Roman Odarchenko, 2018)	AES+ELGamal	• The study presents a hybrid AES and ElGamal algorithm that combines the speed of AES with the security features of ElGamal. • The effectiveness of AES's encryption/decryption speed and ElGamal's improved security characteristics are demonstrated by experimental findings. • The combined AES and ElGamal algorithm shows off a solid solution with increased complexity and vulnerability security. • The proposed hybrid model shows how it might be used in flight control and aviation information security systems, in particular.	• The hybrid algorithm has only been partially investigated in terms of potential flaws and attacks. • Further research is required to determine the hybrid algorithm's performance and scalability in large-scale aviation systems.
4	(H.T. Assafli and I.A. Hashim, 2020)	AES-CBC	• Improves on the previous method's structure by incorporating a Unix time parameter. • More secure than both the original and previously modified AES-CBC algorithms.	• A bit complex when compared to others encryption methods.
5	(Jingjing Zhao, 2023)	DES+RSA	• The DES and RSA encryption algorithms are explained in depth, along with a performance analysis, in the work. • A hybrid encryption method that combines DES and RSA keys improves security without slowing down encryption. • Performance evaluation demonstrates the hybrid algorithm's capacity to provide both increased encryption security and speed. • With the suggested hybrid encryption system, more varied practical applications are now possible.	• The possibility of DES optimization via S-box restructuring is not fully investigated. • To find and investigate many application cases for the hybrid encryption method, more research is needed.

Figure 4 List of researched papers, their findings, and limitations

2.3 Research Gap:

On the market, there are numerous hybrid encryption systems that combine the advantages of symmetric and asymmetric encryption methods to offer a more secure encryption system. Meanwhile, each approach includes flaws and inadequacies that make it vulnerable to particular sorts of attacks. New encryption methods are therefore required that could overcome these constraints and provide an enhanced level of protection and efficacy. The main goal of this research is to determine whether the proposed AES/ECC encryption method improve the security and efficacy of encryption systems and whether they are appropriate for various types of data and applications. With the help of our research, we intend to help secure confidential information and contribute to the advancement of more effective encryption systems.



1	AES+RSA	Hybrid	Faster Encryption using AES, with the security of RSA	Improved encryption speed and security but key management can be complex
2	AES+SHA	Hybrid	Combining encryption and hashing for data integrity	Provides data encryption and integrity, but not suitable for key exchange or digital signatures
3	AES+Blowfish	Hybrid	Combining two symmetric encryption algorithms	Improved encryption strength, but may increase processing time
4	AES+Twofish	Hybrid	Combining two symmetric encryption algorithms	Improved encryption strength, but may increase processing time
5	RSA+Blowfish	Hybrid	Combining asymmetric encryption with symmetric encryption	Improved encryption strength and key management, but may increase processing time
6	RSA+Twofish	Hybrid	Combining asymmetric encryption with symmetric encryption	Improved encryption strength and key management, but may increase processing time

Figure 5 Research Gap

3. Research Methods

3.1 Introduction

The approach used for this study is discussed in this section. It gives information on the methods that were employed, the circumstances, and the software requirements necessary to do this research. This part also discusses the factors that were taken into account for the analysis process, including time and security. It also discusses how the technique was designed, put into practice, and tested.

3.2 Primary and Secondary Sources

Primary research is carefully analysing the response to a research question. Public polls, the development of one's own algorithm, data, observations, etc. may all be used in research rather than relying solely on secondary data. The method of studying an already published research paper in order to strengthen the research's validity is known as secondary research. Articles, books, and other online sources of information are examples of secondary research.

By using his own approach and producing his own results, the researcher employs the main method. The testing platform for the researcher's technique was MATLAB.

The secondary method is used by the researcher to evaluate and contrast the newly developed method with existing methods. Authors use secondary research to analyse various encryption kinds, highlight the limitations of algorithms, and predict what will happen as quantum computing advances.

3.3 Quantitative Research

Quantitative research, according to author Pritha Bhandari(What Is Quantitative Research? | Definition, Uses & Methods, 2020) is the process of obtaining and analysing numerical data. Because of the measurable nature of the factor like CPU performance, time to encrypt/decrypt, avalanche test and cryptanalysis effort, this research employs a quantitative approach. Therefore, this method aids the author in determining whether the methodology was successful in terms of time and data security.

3.4 Procedural approach

A procedural approach is a method for designing, creating, testing, and analysing an algorithm's output. The author's initial steps involved researching the algorithm, determining the strengths and weaknesses of each program, and locating a platform on which to run the algorithm. The author used MATLAB as the testing environment for the methods.

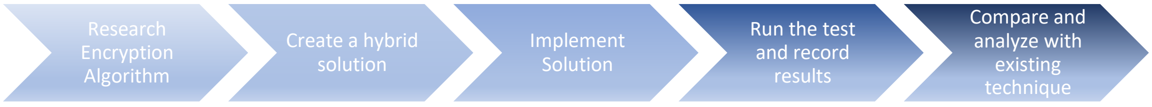

Research Encryption Algorithm
Create a hybrid solution
Implement Solution
Run the test and record results
Compare and analyze with existing technique

Figure 6 Procedural approach for Methods

The author chose the AES and ECC encryption algorithms after first looking into the various encryption algorithms that were available. The selection of these algorithms was made because ECC offers the same level of security with a smaller key than RSA encryption method, while AES is more effective at encrypting huge amounts of data. The researcher came up with three different methodologies and used the mentioned flowchart with each one.

Method 1

In method 1, the solution is to first encrypt the plain text with an AES key and then encrypt the cipher text once again using the ECC encryption algorithm. A speed test and CPU performance comparison with the current hybrid approach were required. Although the above method was superior to other algorithms in terms of security, it was clear from comparisons that it took longer to encrypt because encryption was performed twice. The second approach was developed as a result of the fact that the first method only satisfied one measure, namely security.

Method 2

According to the second technique, we only need to encrypt a portion of the AES key. The AES key is divided into four pieces, and one of those pieces is encrypted using the ECC algorithm. The plain text is encrypted using the new AES key, which was created by combining the encrypted portion with the remaining key. The same environment was used to test the algorithm as method 1 and found out that the encryption time and CPU performance was better than the method 1**.**

Method 3

Since the first method required a lot of time to encrypt and second method required breaking the key then encrypting and again combining, we determined that it would be preferable to first encrypt the AES key with the ECC algorithm before encrypting the plain text with the new AES key. The researcher examined the time and CPU performance using the identical setting as in Method 1 and Method 2. The study observed that it performs better in terms of time and CPU use when compared to method 1 & 2 and other hybrid encryption algorithms that are currently available. Consequently, might be a good choice.

3.5 Software Used

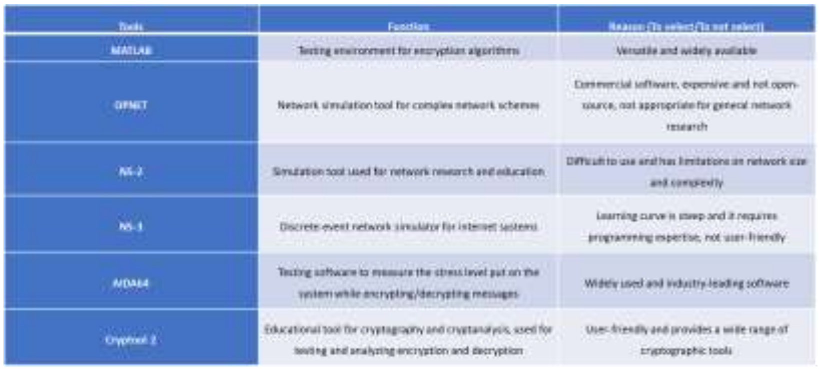
We choose MATLAB for our research after completing in-depth research on a number of testing environments for encryption techniques. This choice is being supported by a number of factors. First off, MATLAB is an effective software suite that offers a variety of tools and functions for testing and assessing 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. We can also learn more about how the encryption methods function thanks to MATLAB's sophisticated visualization and analysis features. Overall, we think MATLAB is a great fit for our research project and will enable us to successfully complete our objectives.

In comparison to programs like NS-2, OPNET, and NS-3, MATLAB will be the most appropriate choice for the experiment because to its accessibility and adaptability. OPNET is a wonderful software, especially for complicated network scenarios, according to research by (Hang Zang et al. 2020), as it gives flexibility and a variety of network simulation models. Additionally, the very simple to learn and use C++ language is offered. However, OPNET is less flexible because it is commercial software and there is no free software accessible. Additionally, the software is pricey, which restricts its user base and makes it more appropriate.

The NS-3 network simulator is a discrete-event network simulator that is employed for network research and testing, claims (Rampfl, 2013). Although it has many advantages, such as good scalability and interoperability with many network protocols, it might not be the best option for testing encryption methods. This is due to NS-3's absence of internal encryption and decryption tools. As a result, significant upgrades and improvements might be needed to implement encryption and evaluate its efficacy. Furthermore, using NS-3 may be challenging for researchers who are unfamiliar with its syntax and structure and requires significant programming expertise.

Another tool we'll use for simulated encryption is called Cryptool 2.

Cryptool 2 is a free and open-source cryptography application, according to (Bruce and Lee, 2014), that provides a variety of cryptographic algorithms and methods for encryption, decryption, and protocol analysis. In order to understand cryptographic principles and evaluate the security of cryptographic systems, academics, students, and professionals regularly use it. Digital signatures, hash functions, symmetric and asymmetric encryption, and other methods are all supported by Cryptool 2.



Tools	Function	Reason (To select/To not select)
MATLAB	Testing environment for encryption algorithms	Versatile and widely available
OPNET	Network simulation tool for complex network schemes	Commercial software, expensive and not open-source, not appropriate for general network research
NS-2	Simulation tool used for network research and education	Difficult to use and has limitations on network size and complexity
NS-3	Discrete-event network simulator for internet systems	Learning curve is steep and it requires programming expertise, not user-friendly
AIDA64	Testing software to measure the stress level put on the system while encrypting/decrypting messages	Widely used and industry-leading software
Cryptool 2	Educational tool for cryptography and cryptanalysis, used for testing and analyzing encryption and decryption	User-friendly and provides a wide range of cryptographic tools

Figure 7 List of tools and their function

3.6 Metrics

For In this research study, two main metrics, time, and CPU performance, were chosen to compare and evaluate the results. The evaluation was based on the AES encryption algorithm, and the NIST standard was used to assess its security and cost.

Time was selected as a crucial factor because it significantly impacts communication efficiency. To measure the time taken for encryption, the researchers utilized the built-in MATLAB Profiler. This profiling method estimates code execution time and identifies the portions of the code that consume the most time.

For evaluating CPU performance, various aspects of the CPU were measured, such as CPU usage and clock speed, using the AIDA64 software.

In addition to time and CPU performance, another metric employed was the avalanche effect test, which gauges the randomness and strength of the encryption.

Overall, the research aimed to comprehensively assess the AES encryption algorithm by considering factors like time efficiency, CPU performance, security against attacks, and the randomness of encryption.

3.7 Analysis

The analysis of the experiment's findings revealed differences in CPU usage and execution times for each approach that was chosen. In the form of bar charts along with the outcome’s tables, the experiment's findings were presented.

4. Design and Implementation

This section will show the step-by-step implementation of the code:

4.1 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.

At Sender’s End:

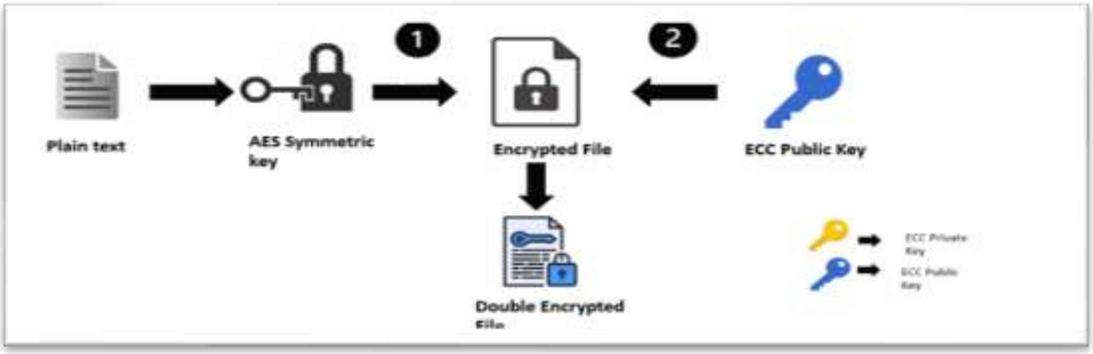


Figure 8 Encryption Process of Method 1

1. Select an unknown plain text that needs to be encoded at the sender's end.

2. With a symmetric key, we will encrypt the selected plain text using the AES technique.

3. Next, encrypt the plain text to obtain our first (initial) cipher text.

4. Using the ECC technique, we will now encrypt the cipher text 1 created in step 3.

5. Our complete encrypted communication is represented by the created text (Cipher text 2).

At Receiver's end:

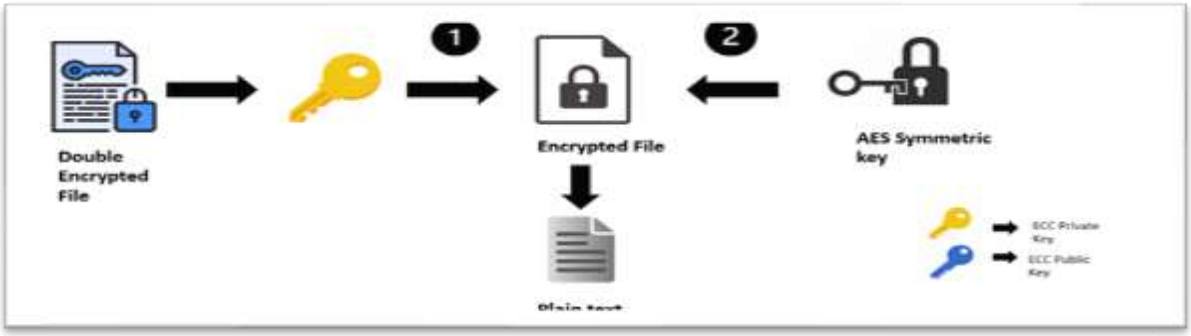


Figure 9 Decryption process of Method 1

1. To decrypt the message, the recipient must first decrypt the cipher text (Cipher text 2) using the ECC technique.

2. Employ the AES algorithm to decrypt the encrypted plain text using the cipher text1.

4.2 Method 2

The second approach divides the AES key into four pieces, one of which is then encrypted with the ECC key. By merging the remaining AES key portion with the encrypted portion, a new AES key is created. The plain text is now encrypted using the new AES key. It is quite similar to the second way, but since we are only encrypting one-fourth of the key, it will take significantly less time and CPU power to do so.

At Sender's End:

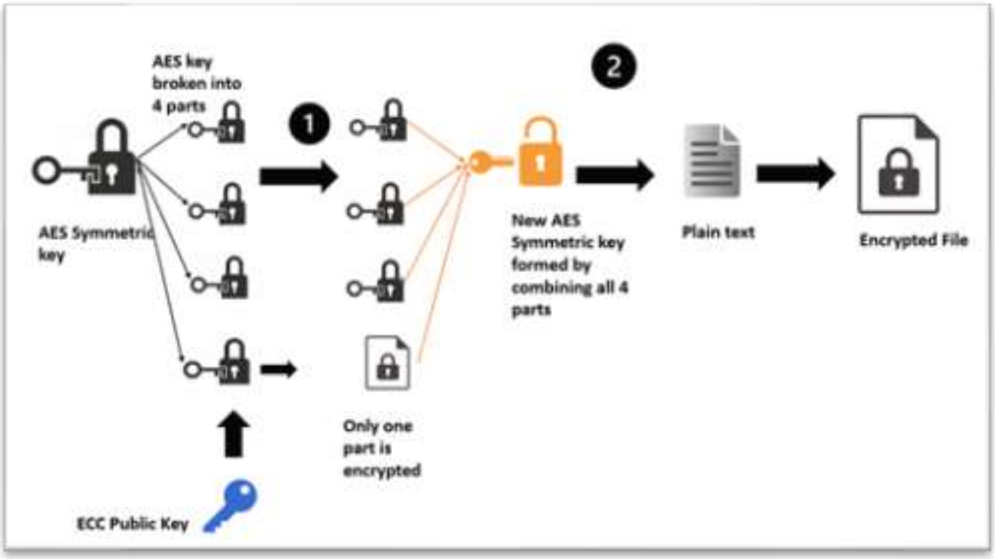


Figure 10 Encryption process of Method 2

1. Pick a piece of plain text that needs to be encrypted at random.

2. Use the AES technique to create a symmetric key.

3. The symmetric key is then divided into a number of pieces, usually four.

4. One AES key fragment is randomly selected and used in the following action.

5. Create a public and private key pair for elliptic curve cryptography.

6. The public key of the ECC key pair is used to encrypt the selected portion of the AES key.

7. The encrypted portion of AES key is attached with the remaining portion of the AES key to form a new AES key.

8. The new AES key is used to encrypt the plain text.

At Receiver's end:

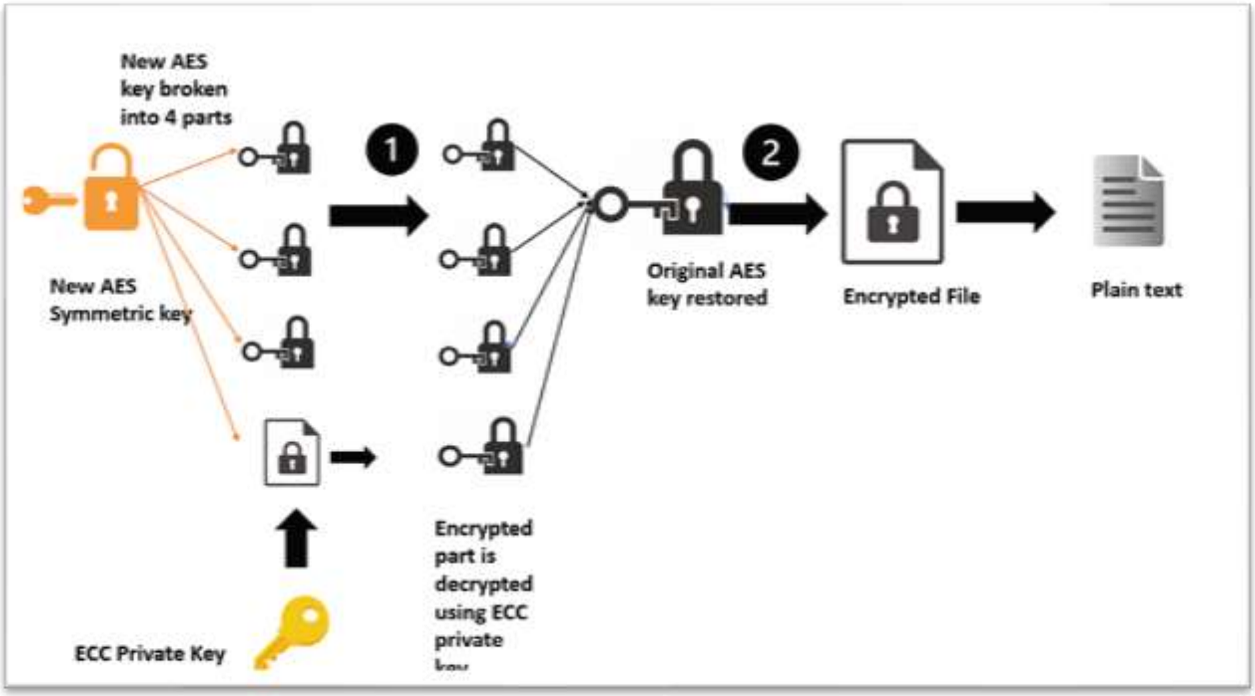


Figure 11 Decryption process for Method 2

1. The recipient decrypts the new AES key piece using their private key connected to the ECC public key after receiving the encrypted ciphertext and ECC public key.

2. The recipient can reassemble the entire AES key by fusing the decrypted piece with the remaining AES key parts.

3. The recipient then uses the rebuilt AES key to decrypt the ciphertext and retrieve the original plaintext.

4.3 Method 3

In the third method, the plain text is encrypted using a new AES key that has been obtained after the AES keys have been encrypted using the ECC technique. In order for the attacker to access the data, he must first decrypt the key.

At Sender's End:

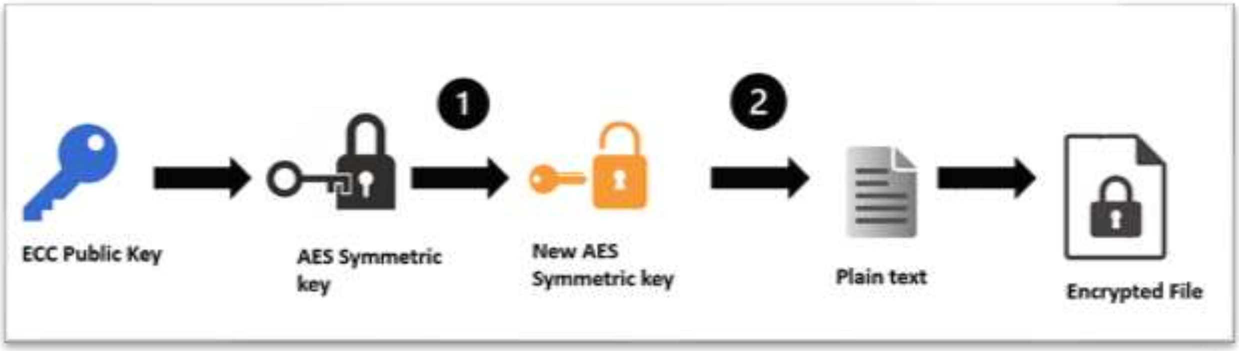


Figure 12 Encryption process for Method 3

1. Select a clear text that requires encryption.

2. generate a private and public ECC key.

3. First, encrypt the AES key using the ECC key.

4. The plain text is encrypted using the received cipher text (new AES key).

At Receiver's end:

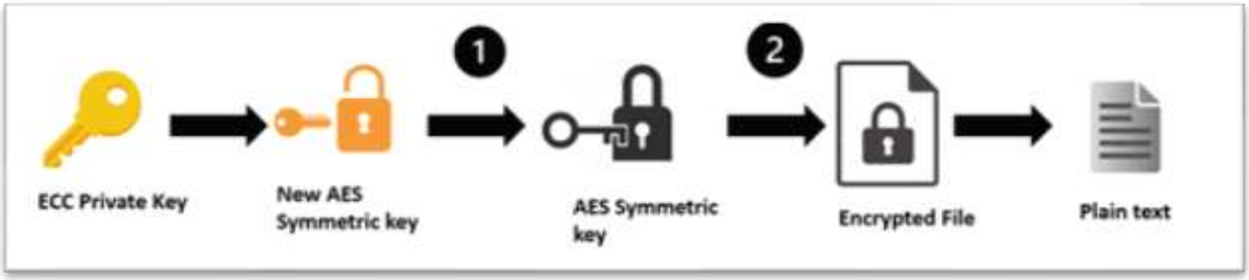


Figure 13 Decryption process for Method 3

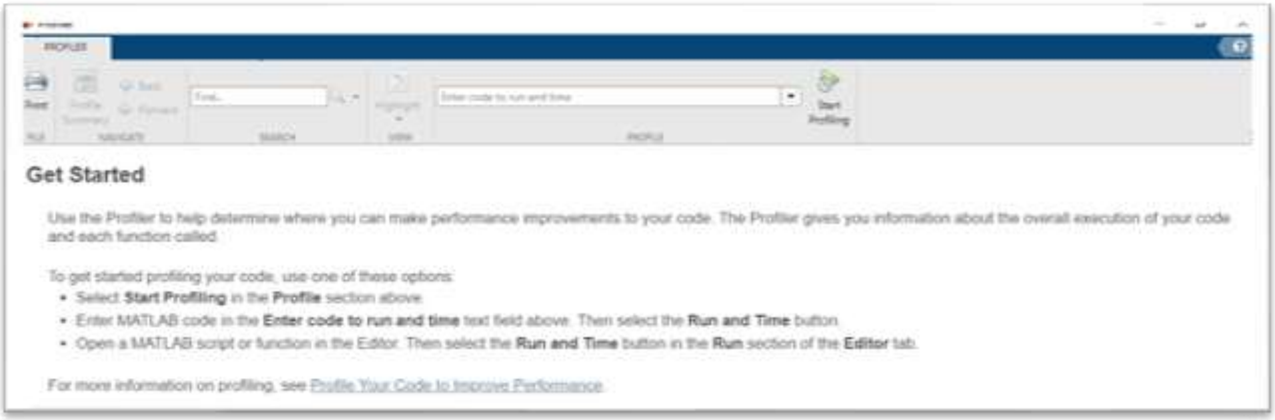
1. To decode the AES key, the recipient uses both their ECC private key and the encrypted AES key.

2. The encrypted plain text can now be decrypted by the recipient using the new AES key.

4.4 Code Analysis:

Profiler:

The MATLAB software's profiler(MATLAB profile - MathWorks) is a tool for measuring and examining the performance of the code. It aids in the identification of coding bottlenecks and inefficiencies, enabling code optimization for faster execution. When we need to enhance the performance of time-consuming MATLAB scripts and functions, profiler is a useful tool.



Get Started

Use the Profiler to help determine where you can make performance improvements to your code. The Profiler gives you information about the overall execution of your code and each function called.

To get started profiling your code, use one of these options:

- Select **Start Profiling** in the **Profile** section above.
- Enter MATLAB code in the **Enter code to run and time** text field above. Then select the **Run and Time** button.
- Open a MATLAB script or function in the Editor. Then select the **Run and Time** button in the **Run** section of the **Editor** tab.

For more information on profiling, see Profile Your Code to Improve Performance.

Figure 14 Profiler Tool in MATLAB

Avalanche Test:

A method for testing cryptographic algorithms called the "Avalanche Test"(Avalanche Effect in Cryptography - GeeksforGeeks) is used to assess a cryptographic algorithm's sensitivity, especially symmetric encryption algorithms like block ciphers. The purpose of the test is to ascertain whether slight modifications to the input data (plaintext) result in appreciable adjustments to the output data (ciphertext).

5. Results and Discussion

We will go into the thorough conclusions drawn from the research undertaken in this section. We will carefully analyse these results, taking into account important parameters like CPU performance, encryption time, and decryption time. These indicators are essential for evaluating the effectiveness and efficiency of the applied encryption algorithms and processes. We can estimate the processing power needed for the encryption and decryption operations by carefully analysing CPU performance.

Time:

The execution time for encrypting and decrypting plain text is shown in Figure 12 in seconds. Execution time contain time of encryption and time for decryption. For the following techniques, time is measured. It is assessed for three distinct messages, which are 16 bytes, 500 bytes, and 1 kilobyte, and for the algorithms RSA, AES, AES+RSA, and AES+ECC(all 3 method). The figure indicates that AES+RSA requires significantly more time to perform encryption and decryption than AES+ECC method.

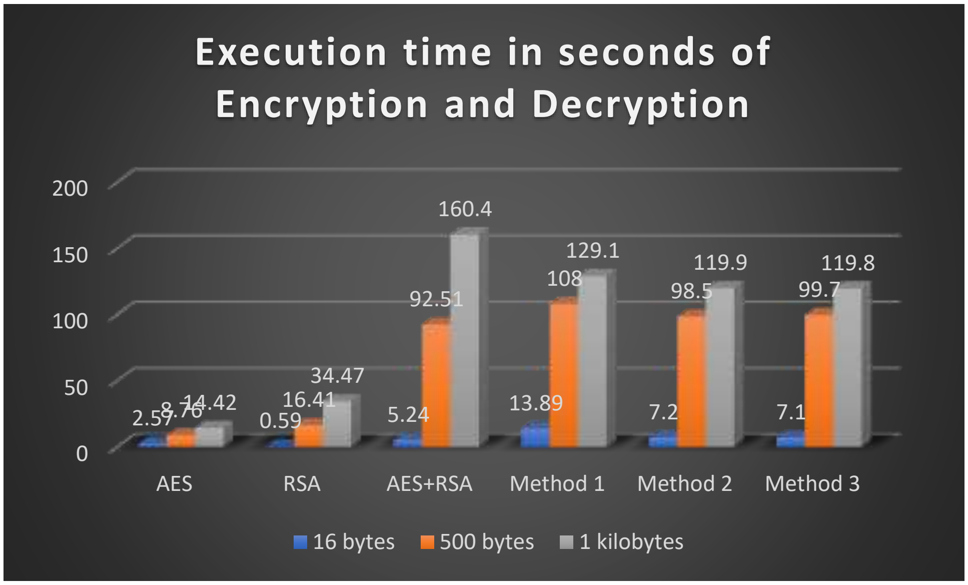
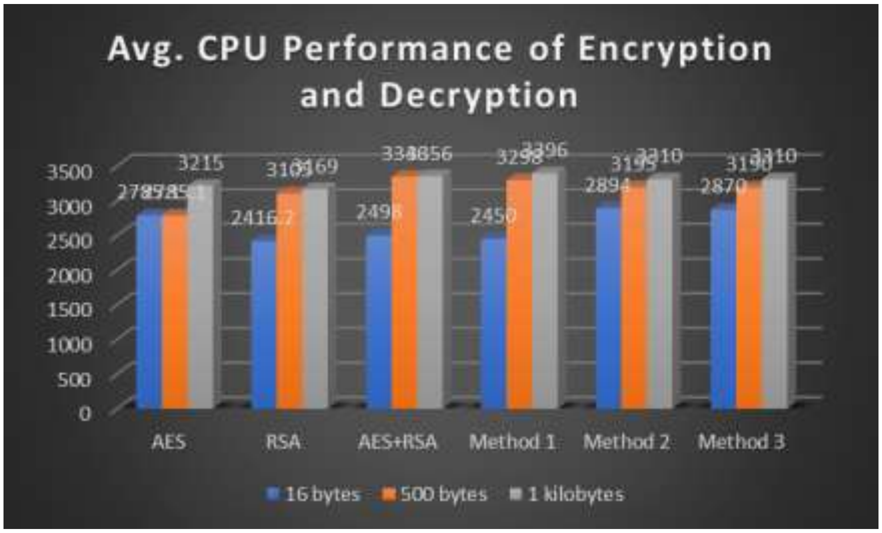


Figure 15 Comparing time taken for Encryption and Decryption by different algorithms.

CPU Performance:

The average CPU clock in Figure 13 illustrates the rate at which each encryption is processed. CPU usage was monitored with the help of AIDA64 Extreme while three separate plaintext messages were encrypted and then instantly decrypted. One kilobyte, 500 bytes, and 16 bytes are these sizes. The figure shows that hybrid AES+RSA method used faster clock speed than AES+ECC algorithm.



.

Figure 16 Comparing CPU Clock for Encryption and Decryption by different algorithms.

Profiler:

A visual representation is shown by profiler which is showing the execution times of various command lines in Figure 17. By highlighting places that may be optimized to increase overall code efficiency and performance, this visualization provides insightful information about the precise lines of code that contribute to process sluggishness.

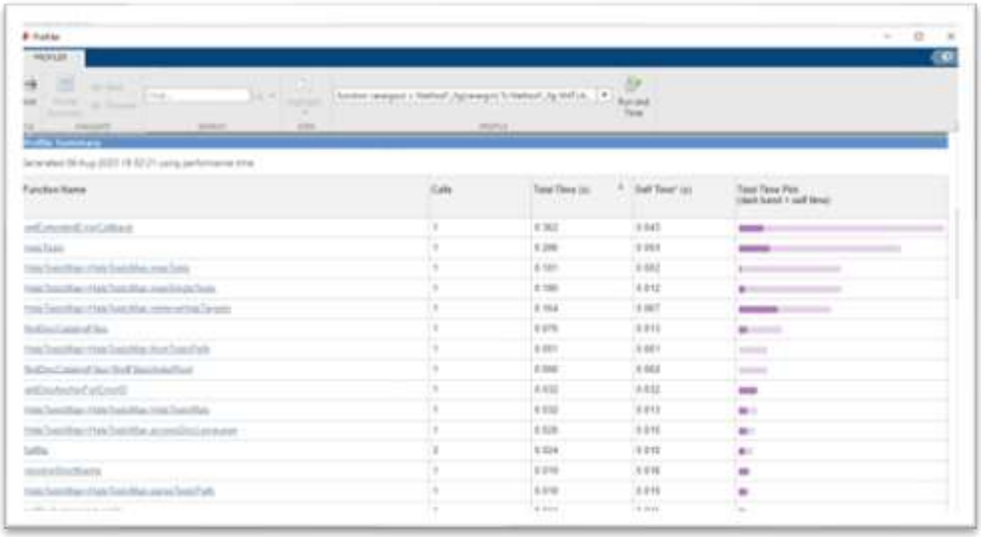


Figure 17 Profiler tool showing time execution of different command lines.

Avalanche Test:

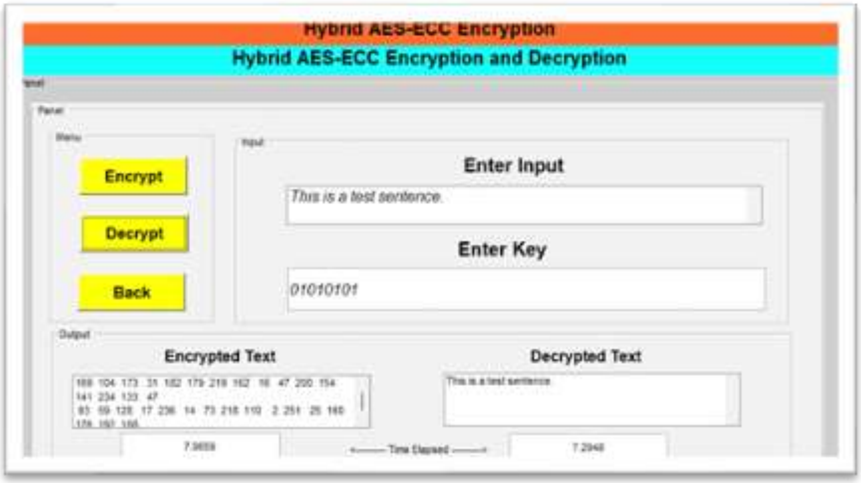
Avalanche tests for the encryption techniques created in this research are shown in figures 15 and 16. The picture illustrates how the cipher text totally changes even when a single digit or character is flipped, demonstrating how high the amount of randomization is.

Plaintext: This is a test sentence.

Key: 01010101

Cipher Text: 169 104 173 31 182 179 219 162 16 47 200 154 141 234 133 47

93 59 128 17 236 14 73 218 110 2 251 25 160 176 192 188


Hybrid AES-ECC Encryption
Hybrid AES-ECC Encryption and Decryption
Panel
Panel
Menu
Encrypt
Decrypt
Back
Input
Output
Time Elapsed

Enter Input

This is a test sentence.

Enter Key

01010101

Encrypted Text

```
169 104 173  31 182 179 219 162  16  47 200 154
141 234 133  47
 83  59 128  17 236  14  73 218 110   2 251  25 160
178 197 168
```

Decrypted Text

This is a test sentence.

7.9659 ← Time Elapsed → 7.2948

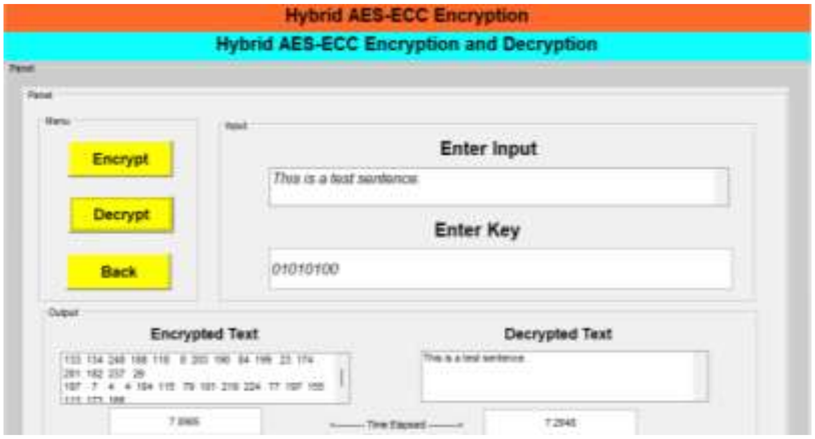
Figure 18 Encryption of plain text with key '01010101'

Now changing the last digit of key from ‘1’ to ‘0’.

Plaintext: This is a test sentence.

Key: 01010100

Cipher Text: 250 67 76 199 145 117 186 149 16 56 205 224 34 64 145 98 77 58 134 193 12 96 190 152 245 183 26 54 174 67 38 54


Hybrid AES-ECC Encryption
Hybrid AES-ECC Encryption and Decryption
Panel
Panel
Menu
Encrypt
Decrypt
Back
Input
Output
Time Elapsed

Enter Input

This is a test sentence.

Enter Key

01010100

Encrypted Text

```
133 134 248 188 118   8 203 190  84 199  23 174
201 182 237  29
187   7   4   4 194 115  79 181 218 224  77 197 155
115 171 188
```

Decrypted Text

This is a test sentence.

7.8965 ← Time Elapsed → 7.2948

Figure 19 Encryption of plaintext with key '01010100'

6. Conclusion and Future Work

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.

Given the results of the study, there are several exciting directions that merit further investigation in the field of future initiatives. Refining the hybrid encryption procedure with a particular focus on reducing execution times while retaining the principles of security and randomness could be one area for additional research. The incorporation of novel quantum cryptographic ideas into the hybrid encryption framework has enormous promise as technology develops. Researchers might work on creating encryption techniques that are resistant to the computing capacity of future quantum computers by addressing the possible difficulties presented by the development of quantum computing. In addition, continual research is necessary to develop encryption techniques that can adapt to changing digital environments and thrive there. Thus, there are many potential to strengthen data security measures and guarantee the confidentiality and integrity of sensitive data in the future landscape of encryption research.

7. References

Agarwal, J., Kumar, M., Srivastava, A.K., 2021. Estimation of Various Parameters for AES, DES, and RSA. Lecture Notes in Networks and Systems 164, 275–283. https://doi.org/10.1007/978-981-15-9774-9_27/FIGURES/6

Al Mamun, S., Mahmood, M.A., Amin, M.A., 2021. Ensuring security of encrypted information by hybrid AES and RSA algorithm with third-party confirmation. Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021 337–343. https://doi.org/10.1109/ICICCS51141.2021.9432174

Assafli, H.T., Hashim, I.A., 2020. Security Enhancement of AES-CBC and its Performance Evaluation Using the Avalanche Effect. 2020 3rd International Conference on Engineering Technology and its Applications (IICETA) 7–11. https://doi.org/10.1109/IICETA50496.2020.9318803

Avalanche Effect in Cryptography - GeeksforGeeks [WWW Document], n.d. URL https://www.geeksforgeeks.org/avalanche-effect-in-cryptography/ (accessed 8.11.23).

Bruce, N., Lee, H.J., 2014. Cryptographic computation of private shared key based mutual authentication protocol: Simulation and modeling over wireless networks. International Conference on Information Networking 578–582. https://doi.org/10.1109/ICOIN.2014.6799747

Hang Zang, Y., Li Wang, Z., Xie, D., Li, J., Gao, H., n.d. Comparison and Analysis of Simulation methods for TSN Performance You may also like Intra-Domain Heuristic Traffic Scheduling Algorithm for Time-Sensitive Networks Comparison and Analysis of Simulation methods for TSN Performance. https://doi.org/10.1088/1757-899X/768/5/052061

Hercigonja, Z., 2016. Comparative Analysis of Cryptographic Algorithms. International Journal of Digital Technology and Economy 1, 127–134.

Iavich, M., Gnatyuk, S., Jintcharadze, E., Polishchuk, Y., Odarchenko, R., 2018. Hybrid Encryption Model of AES and ElGamal Cryptosystems for Flight Control Systems. 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, MSNMC 2018 - Proceedings 127–131. https://doi.org/10.1109/MSNMC.2018.8576289

Journal, I., n.d. Comparative Analysis of Encryption Algorithms Against Text Files.

Li, X., Chen, J., Qin, D., Wan, W., 2010. Research and realization based on hybrid encryption algorithm of improved AES and ECC. ICALIP 2010 - 2010 International Conference on Audio, Language and Image Processing, Proceedings 396–400. https://doi.org/10.1109/ICALIP.2010.5684554

Liu, Y., Gong, W., Fan, W., 2018. Application of AES and RSA Hybrid Algorithm in E-mail. Proceedings - 17th IEEE/ACIS International Conference on Computer and Information Science, ICIS 2018 701–703. https://doi.org/10.1109/ICIS.2018.8466380

Mouha, N., n.d. Review of the Advanced Encryption Standard. https://doi.org/10.6028/NIST.IR.8319

Nadeem, A., Javed, M.Y., 2005. A performance comparison of data encryption algorithms. Proceedings of 1st International Conference on Information and Communication Technology, ICICT 2005 2005, 84–89. https://doi.org/10.1109/ICICT.2005.1598556

Profile execution time for functions - MATLAB profile - MathWorks United Kingdom [WWW Document], n.d. URL https://uk.mathworks.com/help/matlab/ref/profile.html (accessed 8.11.23).

Rampfl, S., 2013. Network Simulation and its Limitations. https://doi.org/10.2313/NET-2013-08-1_08

Rehman, S., Talat Bajwa, N., Shah, M.A., Aseeri, A.O., Anjum, A., 2021. Hybrid AES-ECC Model for the Security of Data over Cloud Storage. Electronics 2021, Vol. 10, Page 2673 10, 2673. https://doi.org/10.3390/ELECTRONICS10212673

What Is Quantitative Research? | Definition, Uses & Methods [WWW Document], n.d. URL https://www.scribbr.com/methodology/quantitative-research/ (accessed 8.11.23).

Zhao, J., 2023. DES-Co-RSA: A Hybrid Encryption Algorithm Based on des and RSA. 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications, ICPECA 2023 846–850. https://doi.org/10.1109/ICPECA56706.2023.10075771