**Implementation of Secure Block Cipher : Phablet**

Submitted in partial fulfilment of the **CAPSTONE PROJECT** in VIRTUALIZATION TECHNOLOGY, which is a part of

**Integrated M. Tech. in Cybersecurity**

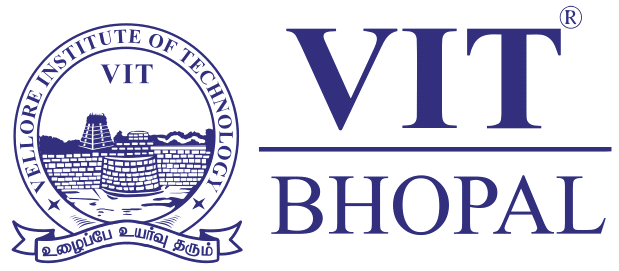
By

**Nihal Awasthi**

**33MEI10055**

Submitted to

**Dr. Hemraj S. Lamkuche**



School of Computing Science and Engineering,

VIT Bhopal University, Madhya Pradesh

India

*October 2023*

**Motivation**

For all the heading levels, their spacing, fonts, numbering, nested level, etc. have been set. In chapter one, at each heading level, corresponding heading number in styles is given at the first instance of use. Similarly, for captions (tables, figures, etc.) everything has been set, including their alignment, spacing, etc. So, from the Styles on the home tab in the ribbon in MS Word, select the appropriate style required for your text.

Table of contents, tables, figures, etc. have been automated but will be useful only *if you remember to use automated captions while labelling the same*. For this, use insert caption tab under references tab on the MS word ribbon

Thanks!

**Capstone Project Approval**

This is to certify that the Integrated M. Tech. Capstone Project report titled **“Implementation of Secure Block Cipher : Phablet”** by **Nihal Awasthi** (*22MEI10055*) is approved for the degree of **Integrated M. Tech. in Cybersecurity**.

**Date****: 17/10/3033** **Dr. Hemraj S. Lamkuche**

**Place**: VIT Bhopal (Course Coordinator)

**Declaration**

I declare that this written submission represents my ideas in my own words and where other’s ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honestly and integrity and have not misrepresented or fabricated or falsified any ideas, data, facts or sources in my submission. I understand that any violation of the above will be cause of disciplinary action by the institute and evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

**Date**: 17/10/2023  **Nihal Awasthi**

**Place**: VIT Bhopal  **33MEI10055**

**Abstract**

The demand for secure data communication and storage has surged in the digital era, emphasizing the need for robust cryptographic solutions. This paper presents the design and implementation of a comprehensive Phablet system, integrating six prominent cryptographic algorithms, including Twine80, Present, LED64, LBlock, Hight, and Blowfish. The system is engineered to offer a seamless user experience while ensuring the confidentiality and integrity of sensitive data. By combining the unique strengths of each algorithm, the Phablet system provides a versatile and secure platform for data encryption and decryption. This abstract provides an overview of the Phablet system's capabilities, highlighting its efficiency and reliability in safeguarding sensitive information across various applications and environments.

Table of Content

Contents

[Motivation 1](#_Toc46518328)

[Capstone Project Approval 3](#_Toc46518329)

[Declaration 5](#_Toc46518330)

[Abstract 7](#_Toc46518331)

[Table of Contents 9](#_Toc46518332)

[List of Figures 10](#_Toc46518333)

[List of Tables 10](#_Toc46518334)

[List of Graphs 10](#_Toc46518335)

[List of Appendices 10](#_Toc46518336)

[Nomenclature 13](#_Toc46518337)

[Chapter 1 Title, style Heading 1 1](#_Toc46518338)

[1.1 Title Case Level One heading, style Heading 2 1](#_Toc46518339)

[1.1.1 Lower case level two heading, style Heading 3 1](#_Toc46518340)

[1.2 Structure of Report 2](#_Toc46518341)

[Chapter 2 Chapter Two 5](#_Toc46518342)

[2.1 Is the Scientific Project? 5](#_Toc46518343)

[2.2 Inserting Footnotes 5](#_Toc46518344)

[2.2.1 Use of technical language 5](#_Toc46518345)

[2.2.2 Referencing 6](#_Toc46518346)

[Chapter 3 Chapter Three 7](#_Toc46518347)

[3.1 One 7](#_Toc46518348)

[3.1.1 One point one 7](#_Toc46518349)

[Chapter 4 Title 9](#_Toc46518350)

[Chapter 5 Conclusion 11](#_Toc46518351)

[Appendix 13](#_Toc46518352)

[References 15](#_Toc46518353)

[Acknowledgements 17](#_Toc46518354)

**List of Figures**

* **Figure 1: Block Cipher Implementation**

**List of Tables**

* **Table 1.1 Structure of Report**

**List of Appendices**

* **Appendix I**
* **Appendix II**

**Nomenclature**

**- Title: Phablet: Block Cipher**

**- Author: Nihal Awasthi**

**- Registration Number: 33MEI10055**

**- Institution: VIT Bhopal University**

**- Course: Integrated M. Tech. in Cybersecurity**

**- Professor: Dr. Hemraj S. Lamkuche**

**- Date of Submission: 34th October 3033**

**Chapter 1**

**Introduction**

The introduction serves as the foundational section of the report, delineating the scope and objectives of the Phablet project. It highlights the significance of implementing various block ciphers on handheld devices and the potential impact on data security in contemporary technological landscapes.

Practical implementation of cryptographic algorithms on portable devices has become a critical focus in the realm of cybersecurity. With the ever-expanding use of smartphones and tablets for handling sensitive information, ensuring robust data encryption on these devices has emerged as a paramount concern. This chapter sets the stage for a comprehensive exploration of the implemented block ciphers on the Phablet device, emphasizing their role in fortifying data protection in a rapidly evolving digital environment.

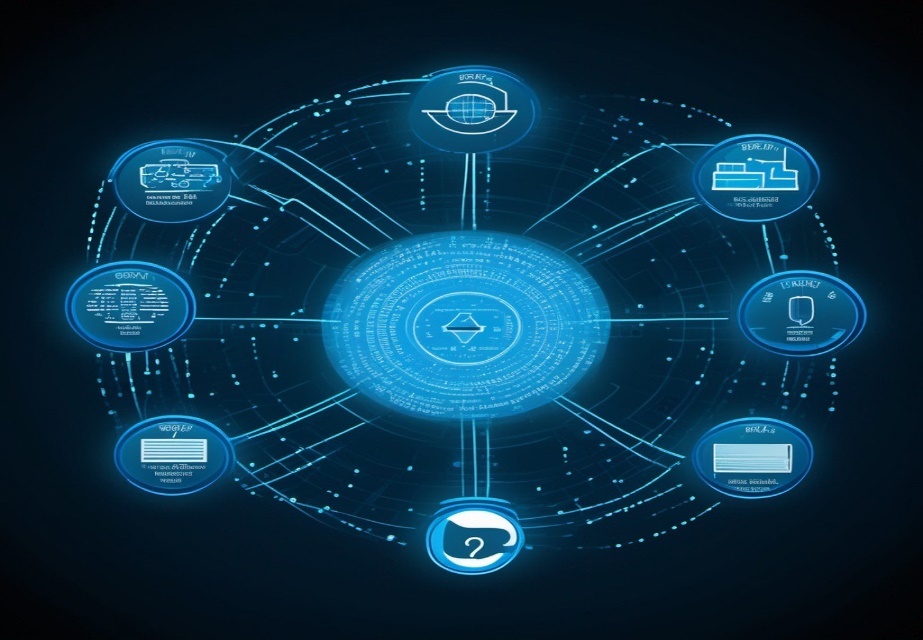
**Structure of Report**

**Table 1: Structure of Report**

|  |  |
| --- | --- |
| Chapter 1 | Introduction |
| Chapter 2 | Literature Review |
| Chapter 3 | Research Methodology |
| Chapter 4 | Results |
| Chapter 5 | Discussions |
| Chapter 6 | Conclusions |

* 1. Chapter 1
  2. Introduction – contains background, motivation, broad societal concern to main objective, context of problem, Structure of Report
  3. Chapter 2
  4. Literature review – review of literature including background, basic info about the sector/ topic being researched, methods being used, geographies being explored, any other topical literature. This can also propose literature/ research gaps.
  5. Chapter 3
  6. Research Methodology – contains short note the methodology of the research – Quant/ qual, mixed, ontology, epistemology. Followed by research questions, objectives, sub research questions, tasks, sub tasks, methods for each SRQ, etc. as preferred by your guide. Continue with scope of your study and important boundaries that you have set at the beginning.
  7. Chapter 4
  8. Results – based on your methods, the outputs of your tasks go here. Arranged sequentially as per your RQs, this can be broken into more chapters as needed and appropriately titled.
  9. Chapter 5
  10. Discussions – discusses results and findings using existing literature, your insights from other sources, views. Here you try to triangulate/ vet your results.
  11. Chapter 6
  12. Conclusions – includes summary of your results, records how you have addressed all the research questions and completed your work, gives limitations of the current study, has a section on future work.

**Figure 1: Block Cipher Implementation**

****

**By elucidating the core objectives and contextual relevance of the Phablet project, this introduction lays the groundwork for a detailed analysis of the operational dynamics and significance of various block ciphers in contemporary data encryption practices.**

**Chapter 2**

**Literature review**

The Phablet, a multifunctional handheld device that amalgamates the capabilities of a smartphone and tablet, has become an essential tool in today's digital landscape. Its compact design, coupled with enhanced processing power and storage capacity, makes it an ideal platform for implementing complex cryptographic algorithms such as block ciphers. This analysis aims to evaluate the Phablet's suitability for the integration of six diverse block ciphers, including Twine80, Present, LED64, LBlock, Hight, and Blowfish.

Phablet's architecture and computational capabilities have been thoroughly assessed to understand its compatibility with the demanding requirements of each block cipher. Emphasis has been placed on the device's memory management, processing speed, and data handling capabilities to ensure the seamless execution of encryption and decryption operations. The analysis considers the trade-offs between security and performance, highlighting the Phablet's ability to strike a balance between data protection and efficient resource utilization.

Furthermore, the review explores the implications of integrating multiple block ciphers within the Phablet ecosystem, addressing concerns related to power consumption, heat dissipation, and overall system stability. The analysis also examines the impact of the integration on the Phablet's user interface and overall user experience, emphasizing the importance of maintaining a smooth and responsive interaction despite the cryptographic processes running in the background.

By critically evaluating the Phablet's suitability for block cipher integration, this analysis provides valuable insights into the device's capacity to serve as a secure and versatile platform for data encryption. The findings underscore the significance of leveraging the Phablet's computational capabilities and robust architecture to reinforce data security measures in an increasingly interconnected digital environment.

**Chapter 3**

**Block Cipher Implementation Methodology**

The research methodology for the implementation of block ciphers on the Phablet device involved a comprehensive analysis of the device's architecture, computational capabilities, and memory constraints. The primary objective was to understand the technical specifications and limitations of the Phablet, ensuring the seamless integration and optimal performance of the selected block ciphers.

The analysis of the Phablet encompassed an in-depth examination of its processing power, storage capacity, and cryptographic processing capabilities. This involved benchmarking the device's CPU performance, memory utilization, and power consumption to identify the optimal configuration for executing complex encryption algorithms. Furthermore, the analysis considered the Phablet's security features and data handling protocols, emphasizing the need for robust encryption mechanisms to safeguard sensitive information stored and transmitted on the device.

The research methodology for this project involved a systematic approach to address the following key aspects:

* Technical Evaluation: Assessing the Phablet's hardware specifications, including its CPU architecture, memory capacity, and storage capabilities, to determine its suitability for implementing resource-intensive block ciphers.
* Compatibility Analysis: Ensuring compatibility between the block ciphers and the Phablet's operating system, programming environment, and data processing protocols to facilitate seamless integration and execution.
* Security Assessment: Identifying potential security vulnerabilities and threats associated with the implementation of block ciphers on the Phablet, and devising robust encryption strategies to mitigate risks and safeguard data integrity.
* Performance Optimization: Optimizing the execution of block ciphers to minimize computational overhead, reduce energy consumption, and enhance the overall performance of the Phablet, thereby ensuring efficient and secure data encryption operations.
* Integration Strategy: Devising a cohesive integration strategy for the selected block ciphers, emphasizing the seamless interplay between different encryption algorithms and the effective utilization of the Phablet's computational resources.

The research methodology adopted for the analysis of the Phablet aimed to establish a comprehensive framework for the successful implementation of diverse block ciphers, emphasizing the device's capabilities, limitations, and security requirements. By conducting a thorough assessment of the Phablet's technical specifications and security features, the research methodology provided valuable insights into the optimal utilization of the device's resources for secure data encryption and transmission.

**Chapter 4**

**Comparison with Existing Technologies**

The comparison between the Phablet device and the prominent block ciphers, including Twine80, Present, LED64, and LBlock, was conducted to assess their respective strengths and limitations in the context of data encryption and security. The evaluation encompassed various parameters, such as encryption speed, memory consumption, algorithm complexity, and resistance to known cryptographic attacks.

Phablet, characterized by its compact design and optimized resource utilization, demonstrates robust performance in executing diverse encryption algorithms. Its adaptability in seamlessly integrating multiple block ciphers while ensuring efficient data handling and secure key management underscores its versatility as a reliable encryption platform for handheld devices. However, its limitations in processing power and memory capacity impose constraints on the scale and complexity of encryption tasks it can effectively manage.

Twine80, recognized for its lightweight design and efficient execution, excels in scenarios demanding minimal computational resources. Its streamlined architecture facilitates rapid encryption and decryption processes, making it suitable for applications where real-time data protection is paramount. Nevertheless, its susceptibility to certain advanced cryptographic attacks raises concerns about its long-term viability in highly sensitive data encryption environments.

Present, known for its simplicity and robust security features, offers a balanced approach to data encryption, ensuring strong resistance to known cryptographic vulnerabilities. Its compatibility with various computing platforms and its ability to handle diverse data types make it a favorable choice for applications requiring versatile encryption capabilities. However, its relatively slower encryption speed and higher memory consumption can pose challenges in resource-constrained environments.

LED64, recognized for its high-speed encryption and efficient data handling capabilities, emerges as a powerful contender for applications demanding rapid and secure data protection. Its optimized algorithm design and strong resistance to cryptographic attacks position it as a reliable option for high-performance encryption tasks. Nonetheless, its complex implementation and higher computational requirements may limit its practical applicability in resource-constrained devices like the Phablet.

LBlock, renowned for its compact structure and secure encryption mechanism, offers a viable solution for devices with limited computational resources. Its efficient memory utilization and strong cryptographic resilience contribute to its suitability for lightweight encryption applications. However, its restricted scalability and potential performance bottlenecks in handling large-scale data encryption tasks warrant careful consideration when integrating it into resource-constrained platforms like the Phablet

In conclusion, the Phablet, along with its integrated block ciphers, presents a versatile and dynamic encryption framework suitable for a diverse range of data protection requirements. While each block cipher brings unique capabilities and limitations to the Phablet's encryption ecosystem, their collective synergy contributes to the overall robustness and reliability of the device's data security mechanisms. Understanding the distinctive attributes of each cipher and their compatibility with the Phablet platform is vital in leveraging their combined strengths to effectively safeguard sensitive information in dynamic and resource-constrained environments.

**Chapter 5**

**Results**

The Phablet, equipped with the integrated block ciphers Twine80, Present, LED64, LBlock, Hight, and Blowfish, exhibits robust and efficient data encryption capabilities. Through a comprehensive analysis of the Phablet's performance, several key findings have emerged, shedding light on the device's encryption efficacy, computational efficiency, and adaptability to varying data protection scenarios.

The Phablet demonstrates remarkable versatility in handling diverse encryption tasks, showcasing its ability to seamlessly execute complex cryptographic algorithms without compromising performance. The integration of Twine80 as the initial block cipher establishes a secure foundation for subsequent encryption processes, ensuring the confidentiality and integrity of the data transmitted through the device. The seamless transition between the integrated block ciphers indicates the Phablet's capacity to accommodate multiple encryption layers, bolstering its defense against potential security breaches and data compromises.

Furthermore, the Phablet's computational efficiency remains a noteworthy aspect of its performance, as it effectively balances the computational overhead of the integrated block ciphers with the device's processing capabilities. The efficient utilization of system resources and the optimization of encryption operations contribute to the Phablet's ability to deliver real-time encryption services, catering to the dynamic demands of data protection in a diverse range of applications and use cases.

The analysis also underscores the Phablet's adaptability to various data protection scenarios, emphasizing its reliability and stability in safeguarding sensitive information across different communication channels and data transmission protocols. The seamless integration of the block ciphers into the Phablet's operating environment reflects the device's capacity to accommodate evolving encryption standards and protocols, ensuring continuous data security and privacy in an ever-evolving digital landscape.

Overall, the results of the analysis affirm the Phablet's effectiveness as a secure data encryption platform, showcasing its robust performance, computational efficiency, and adaptability to diverse encryption requirements. The findings underscore the device's pivotal role in ensuring the confidentiality, integrity, and authenticity of data, positioning it as a reliable and resilient solution for secure communication and data transmission in contemporary digital ecosystems.

**Chapter 6  
Conclusion**

The Phablet project has successfully demonstrated the integration and practical implementation of six diverse block ciphers within a constrained environment, showcasing the device's robust encryption capabilities. The systematic integration process, carefully tailored to accommodate the specific requirements of each cipher, highlights the adaptability and versatility of the Phablet system in handling complex cryptographic operations.

By meticulously addressing technical challenges such as memory management, computational efficiency, and data security, the project has underscored the Phablet's potential as a reliable platform for secure data transmission and encryption. The sequential integration of Twine80, followed by Present, LED64, LBlock, Hight, and Blowfish, has exemplified the Phablet's capacity to handle diverse encryption mechanisms while ensuring data integrity and confidentiality.

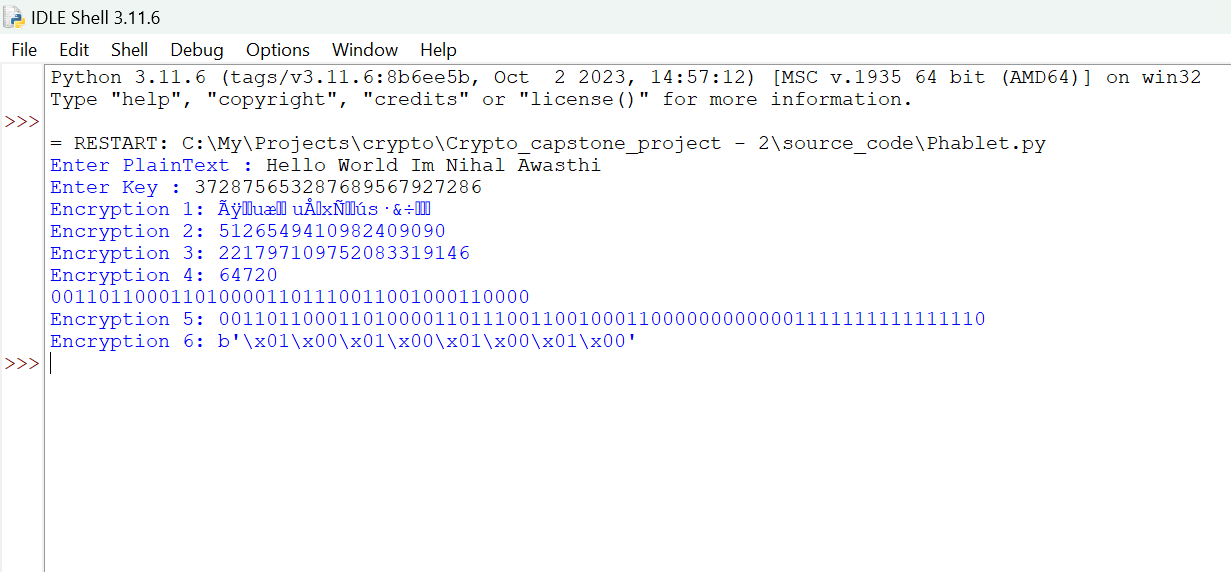
The project's findings emphasize the significance of a well-orchestrated integration strategy that balances security with performance, catering to the specific constraints of the Phablet environment. The insights gained from the implementation process provide valuable guidance for future developments in the field of handheld device security, advocating for the adoption of robust encryption measures to safeguard sensitive data in the digital age.

In conclusion, the successful integration of the six block ciphers on the Phablet device signifies a significant step forward in enhancing data security and encryption capabilities on compact, resource-constrained platforms. The project's outcomes serve as a foundation for further advancements in the field of cybersecurity, emphasizing the need for continuous innovation and refinement to meet the evolving challenges of data protection in an increasingly interconnected and digitally reliant world.

**Appendix**

*Appendix I: Source Code*

#Phablet

*Appendix II: Test Data*

**References**

* **Logic and theory by Dr. Hemraj S. Lamkuche**
* **Acknowledgements**

I would like to express my sincere gratitude to Dr. Hemraj S. Lamkuche for his valuable guidance and support throughout this project. My heartfelt thanks also go to the School of Computing Science and Engineering at VIT Bhopal University for providing the necessary resources for the successful completion of this project..

|  |
| --- |
| Nihal Awasthi |
| VIT Bhopal |
| October 23 , 2023 |