Mobile-based Learning Application for Enhancing Understanding of Cipher Feedback Algorithms

Amar Al Fatah
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
At the Information Technology Study Program of Universitas Ahmad Dahlan, Yogyakarta, cryptography is a core subject in the computer security course. Due to limited lecture time, cryptographic algorithms such as Cipher Feedback cannot be discussed in depth. This research aims to develop an Android application focused on the Cipher Feedback algorithm. The development process involves collecting data from Android-using students, literature study, observing cryptographic programs, and designing and implementing the application using Kotlin. The application is tested using Black Box Testing and the System Usability Scale to ensure its functionality. The results are expected to help students understand encryption and decryption using the Cipher Feedback algorithm.

Keywords
Learning Application, Mobile, Cryptography, Cipher Feedback, Waterfall.

1. INTRODUCTION
The rapid advancement of technology in the digital era has significantly transformed the way people interact and conduct their daily activities. One of the most prominent aspects of this transformation is the widespread use of smartphones. According to data from Newzoo, there were approximately 192.15 million smartphone users in Indonesia in 2022 [1]. Additionally, mobile application usage has experienced substantial growth, with a total of 7.7 billion app downloads [2] and users spending an average of 5.7 hours using mobile apps in 2022 [3]. With increasingly sophisticated capabilities, smartphones have evolved beyond mere communication tools to become hubs for information, entertainment, and productivity for society. However, alongside these benefits, technological advancements also bring new challenges, particularly in the form of cybercrime.

In this context, cybercrime cases are on the rise alongside the widespread use of technology. According to Databoks [4], there were 182 reported cases of data theft, indicating a 27.3% increase from the previous year's 143 reports. Over the past five years, incidents of data theft have surged by 810% from a mere 20 cases. Cybercriminals exploit vulnerabilities in technology systems and internet networks to pilfer personal data or compromise accounts, posing serious threats to the privacy and security of individuals and institutions alike. As technology advances, so too does the sophistication of cyber threats, necessitating robust measures to safeguard sensitive information and combat digital crimes effectively.

The integration of technology into education has driven the rise of mobile learning applications, offering flexibility and accessibility for learners. However, this shift also introduces cybersecurity risks, highlighting the need for interactive and secure learning platforms that protect data privacy while enhancing the learning experience.

Data security is a critical issue because it involves the protection of sensitive data from unauthorized access, alteration, or deletion [5]. Key aspects of data security include authentication, confidentiality, integrity, and non-repudiation. These aspects can be addressed using cryptographic techniques [6]. Cryptography is a method used to secure data by encrypting it, making it difficult for unauthorized individuals to access or read the information without the appropriate decryption key [7]. In essence, cryptography transforms readable data into seemingly random content [8].

In the academic setting, particularly within computer science departments, various courses such as computer security and cryptography are offered. One topic that is often challenging for students to grasp is the concept of block cipher. Within block ciphers, one notable mode is Cipher Feedback (CFB). CFB encrypts data in smaller units than the block size of the key and operates using a Shift Register system. At the start of the process, the Initialization Vector is encrypted with a key [9]. CFB is a symmetric algorithm that uses a single key for both encryption and decryption [10].

To address this educational challenge, the Cipher Feedback (CFB) algorithm learning application has been developed. This mobile application serves as a tool for teaching encryption and data security, providing users with a clear understanding of data protection and its importance in the digital era. By leveraging technology, this application aims to foster greater comprehension of encryption techniques while ensuring that sensitive information remains secure.

2. RELATED WORKS
Hendy and Habibullah Akbar (2021) developed an Android application titled "Belajar Kriptografi" as an educational tool for cryptography courses. The application was built using the Rapid Application Development (RAD) approach and covered cryptography topics such as XOR operations, ASCII conversion, Caesar Cipher, Vigenere Cipher, and RSA encryption. The testing phase showed an average System Usability Scale (SUS) score of 73.255%, with expert approval ratings surpassing 80% and user satisfaction exceeding 70%. The application was deemed successful in supporting students' comprehension of cryptography concepts [11].

Harvei Desmon Hutahaean and Paska Marto Hasugian (2019) developed a mobile-based cryptography learning application using the Computer Assisted Instruction (CAI) method. This application aimed to assist students in grasping data security techniques, particularly focusing on the RC5 algorithm. The platform featured tutorials, exercises, simulations, and educational games to explain encryption and decryption processes with RC5. Research findings indicate that the CAI method successfully increased interactivity and enhanced learning outcomes, promoting greater interest and understanding of data security [12].

Siti Hajar (2019) created educational software for the Electronic Code Book (ECB) algorithm using the CAI method. The objective was to improve students' understanding of ECB encryption through interactive tutorials and exercises. ECB divides plaintext into blocks, which are encrypted independently. This software was specifically developed for desktop platforms and utilized multimedia elements such as visualizations, audio, and animations to reinforce key concepts [13].

Riska Oktaria (2019) developed a cryptography learning application utilizing the CAI method, focusing on the Data Encryption Standard (DES) algorithm. The application integrated tutorials, simulations, and interactive exercises to facilitate students' understanding of encryption and decryption techniques within DES. Multimedia elements like Macromedia Flash were employed to present engaging and interactive learning materials, showcasing the significant role of multimedia in enhancing cryptographic education [14].

Muhammad Fauzi Dalimuthe (2019) designed an application for securing text documents using the Cipher Feedback (CFB) algorithm. The CFB algorithm encrypts data by processing it in smaller units than the block size and employs a shift register system. The developed application implements both encryption and decryption processes, producing ciphertext and plaintext as respective outputs. The research demonstrated the application's effectiveness in securing text documents using the CFB algorithm, with potential for integration into broader information systems to enhance data protection [15].

3. METHODOLOGY

The methodology of this research is designed to systematically develop a mobile-based learning application for the Cipher Feedback (CFB) algorithm. This application aims to enhance the understanding of cryptographic principles among mobile users, facilitating flexible learning environments. The data collection methods utilized in this study are grounded in objective recording and gathering of relevant information [16]. The approach consists of two main methods: literature review and observation.

a. *Literature Review*
A comprehensive literature review was undertaken to gather existing knowledge on cryptographic algorithms and mobile learning platforms. This review involved exploring a diverse array of sources, including academic journals, conference proceedings, theses, and reputable online materials. The primary objective of the literature review was to identify gaps in current educational tools for cryptography and to inform the development process of the mobile application. Specific attention was paid to previously established methodologies, pedagogical strategies, and technological innovations that have been employed in the domain of mobile learning. This analysis helped shape the application's content and features to meet the educational needs of users effectively.

b. *Observation*
Observational studies were conducted within educational settings to gain insights into the challenges students face in comprehending cryptographic concepts, particularly those related to block ciphers. These observations focused on students' interactions with existing learning materials and their engagement levels during lectures and practical exercises. By documenting instances where students struggled to grasp key concepts, the research team was able to pinpoint specific difficulties that needed to be addressed in the application design. This foundational understanding was crucial for creating a user-centric learning tool that responds to actual learner needs.

The development of the mobile application employed a variety of system development methodologies, including waterfall, prototype, Rapid Application Development (RAD), agile, iterative, and spiral models. After careful consideration of these methodologies, the Waterfall System Development Method was selected for this study due to its structured and sequential approach. This method ensures that each stage is thoroughly completed before proceeding to the next [17]. The systematic nature of the Waterfall approach allows for a strong emphasis on the quality of each component of the application, making it particularly suited for educational tools where clarity and reliability are paramount [18]. The stages of the Waterfall methodology include:

The stages of the Waterfall methodology include:

a. *Analysis*
Requirements were gathered from user feedback and literature insights, establishing a clear understanding of the necessary functionalities.

b. *Planning*
A project plan was created to outline the development timeline, resource allocation, and milestone targets, ensuring stakeholder alignment.

c. *Implementation*
The application was developed based on design specifications, integrating interactive simulations and quizzes to enhance learning.

d. *Testing*
A comprehensive testing phase evaluated the application's functionality and usability through black box and user acceptance testing, identifying potential issues before release [19].

e. *Maintenance*
Post-deployment, the application will undergo ongoing maintenance to incorporate user feedback, update content, and improve functionalities.

The detailed stages of the Waterfall method are illustrated in Figure 1, providing a visual representation of the structured approach taken in this research.

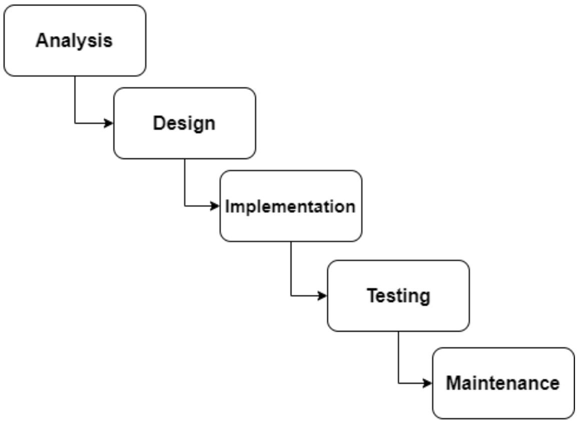

Figure 1: Waterfall Method

3.1 System Requirement Analysis

This research aims to create a mobile-based Android application specifically designed to teach encryption and decryption processes using the Cipher Feedback method. Targeting Computer Science students, especially those enrolled in computer security or cryptography courses, the application seeks to provide a comprehensive toolset for enhancing their understanding of cryptography. Additionally, it aims to cater to a broader audience interested in exploring cryptographic techniques and their practical applications.

3.1.1 Functional Requirement

Functional requirements specify the capabilities that the software system must provide, derived from user inputs to build and evaluate the software architecture [20]. The functional requirements for this application include:

- *a.* The system must provide study materials and exercises related to the topic.
- *b.* The system must be able to display simulations of the encryption and decryption processes.
- *c.* The system must offer quizzes to assess user understanding and display quiz results.
- d. The system must encrypt data, allowing users to input plaintext, an encryption key, and an initialization vector.
- *e.* The system must decrypt data, allowing users to input ciphertext, a decryption key, and an initialization vector.

3.1.2 Non Functional Requirementl

Non-functional requirements for the learning application using the Cipher Feedback method on Android include:

- a. The system must operate smoothly on the Android platform, ensuring a seamless user experience without significant lag.
- b. The system must be compatible with various Android versions, starting from version 6 (API level 23) and above, to ensure accessibility for a wide range of users.
- c. The user interface must be well-designed for easy comprehension and usability.
- d. The system should include guides to assist users in utilizing all available features.

3.2 System Design

This section outlines the steps involved in developing the Mobile-Based Cipher Feedback Algorithm Learning Application.

3.2.1 Flowchart Design

Flowcharts are graphical analysis tools used to clearly and logically depict various aspects of information systems. They document the execution of business processes and the flow of information within an organization [21].

a. Encryption Flowchart for Cipher Feedback

The CFB encryption process begins by converting the plaintext and key into binary form and splitting the plaintext into 8-bit blocks. The process involves encrypting the Initialization Vector (IV) using key K, applying XOR, and a 1-bit left shift to generate the most significant bit (MSB). This MSB is then XORed with the plaintext block Pi to produce the ciphertext Ci. If Pi is not the last block (Pn), Ci is fed back into the least significant bit (LSB) for the next iteration. This process concludes after processing the final block. This flow is illustrated in Figure 2.

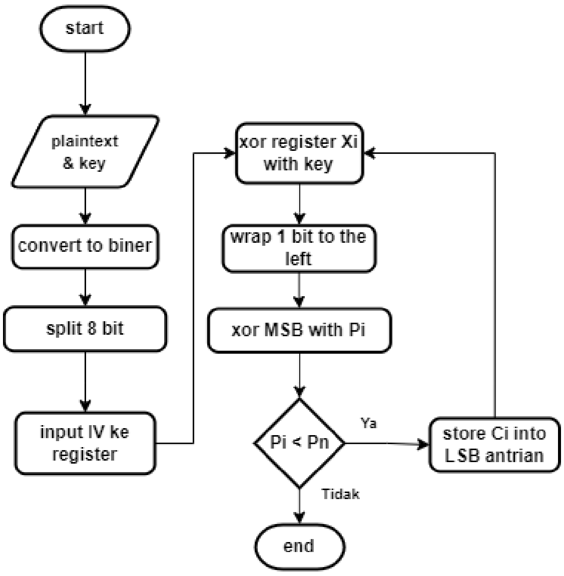

Figure 2: Encryption Flowchart CFB

b. Decryption Flowchart for Cipher Feedback

The CFB decryption process starts with the ciphertext and key in binary form, divided into 8-bit blocks. The decryption begins by encrypting the IV with key K, using XOR and a 1-bit left shift to generate the MSB. This MSB is XORed with the ciphertext block Ci to retrieve the plaintext block Pi. If Ci is not the final block (Cn), it is fed back into the LSB for the next operation. This process is visually represented in Figure 3.

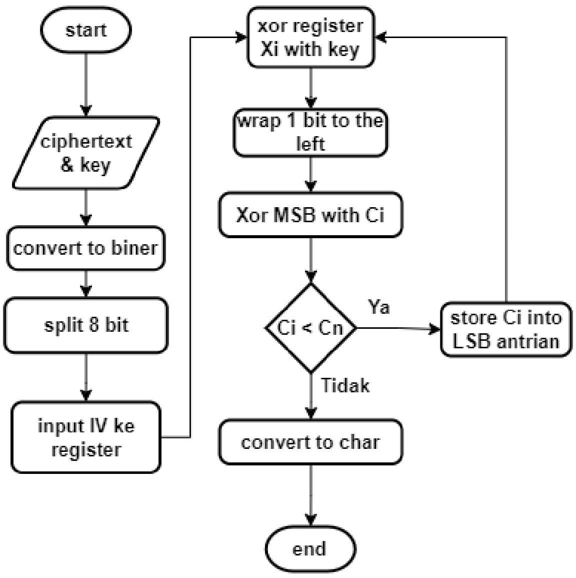

Figure 3: Decryption Flowchart CFB

c. Flowchart for Retrieving Data from Firebase

The flowchart for retrieving data from Firebase begins with initializing a connection to Firebase, followed by creating a reference to the real-time database or Firebase Storage, depending on the data type. A listener is then added to monitor real-time data changes. Upon receiving the data, the system processes it and updates the user interface (UI) accordingly. This design is detailed in Figure 4.

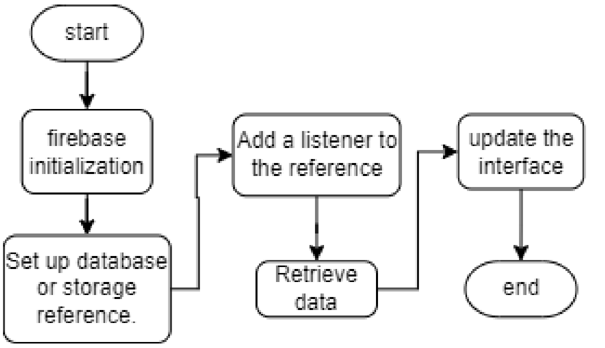

Figure 4: Flowchart for Retrieving Data from Firebase

3.2.2 Use Case Diagram Design

The Use Case Diagram (UCD) models the interactions between users and the mobile learning application, highlighting key functions such as accessing materials and participating in simulations. This diagram, shown in Figure 5, outlines the roles of students, instructors, and administrators, ensuring the application effectively meets user needs. By visualizing these interactions, the UCD aids in identifying system requirements and potential areas for improvement.

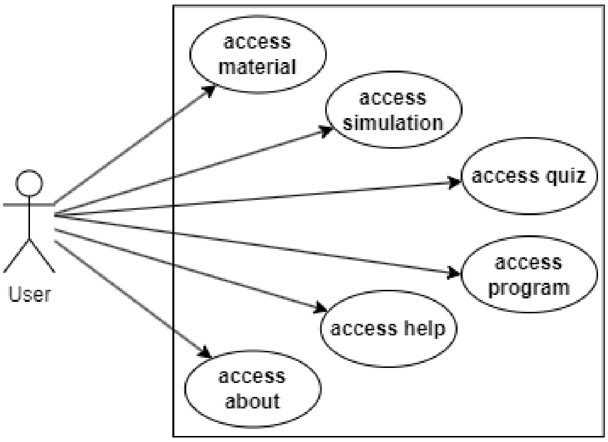

Figure 5: Application Use Case Diagram

3.2.3 Activity Diagram Design

Activity Diagrams visualize workflows and actions within use cases, illustrating the sequence of steps involved [18].

a. Accessing the Material Menu

Figure 6 outlines the process of accessing materials, starting with entering the application, displaying the menu, and selecting the 'Materi' option to present the desired material.

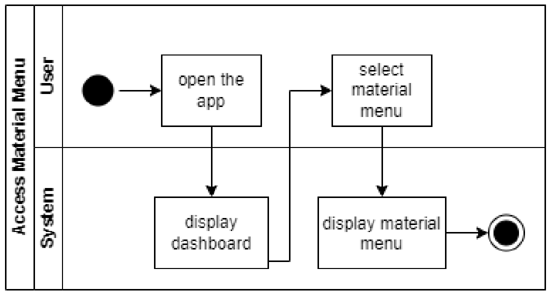

Figure 6: Accessing Material Menu Activity

b. Accessing the Simulation Menu

Figure 7 depicts the process for accessing simulations, beginning with entering the application, selecting the 'Simulasi' menu, and retrieving data from Firebase to update the display.

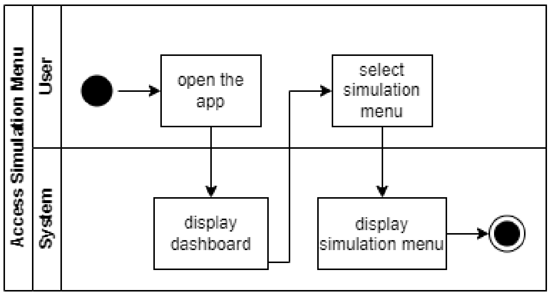

Figure 7: Accessing Simulation Menu Activity

c. Accessing the Quiz Menu

Figure 8 illustrates the process for accessing quizzes, commencing with entering the application, selecting the 'Kuis' menu, fetching quiz data from Firebase, and presenting the results post-quiz completion.

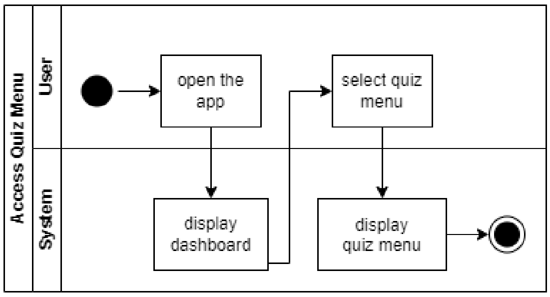

Figure 8: Accessing Quiz Menu Activity

d. Accessing the Program Menu

Figure 9 outlines the procedure for accessing various programs, starting with entering the application, selecting the 'Program' option, and processing user input to display results.

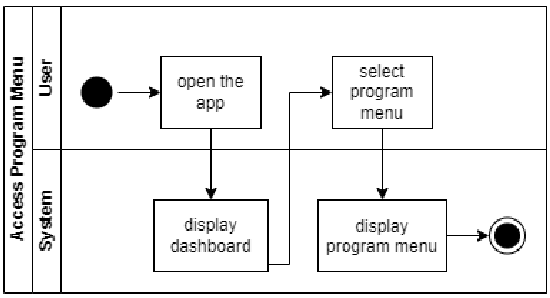

Figure 9: Accessing Program Menu Activity

e. Accessing the Help Menu
Figure 10 illustrates the steps to access the guide within the application. Users start by entering the application and then selecting the 'Panduan' menu option. This menu provides access to a comprehensive guide designed to assist users in understanding various features and functionalities of the application. The clear layout and detailed instructions facilitate easy navigation, ensuring that users can quickly find the information they need to enhance their learning.

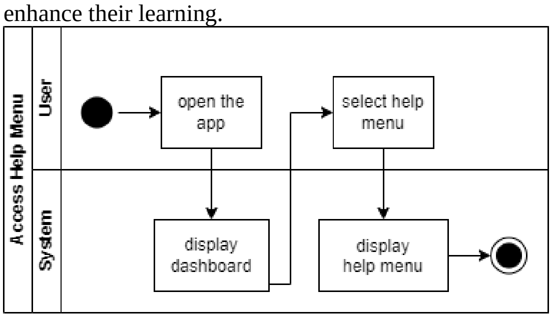

Figure 10: Accessing Guide Menu Activity

f. Accessing the About Menu
Figure 11 describes the procedure for accessing the 'About' menu. Users initiate this process by entering the application and selecting the 'Tentang' menu option. This menu displays relevant information about the application, including its purpose, main features, and details about the development team. By providing this information, users gain a better understanding of the application's objectives and the context in which it was developed.

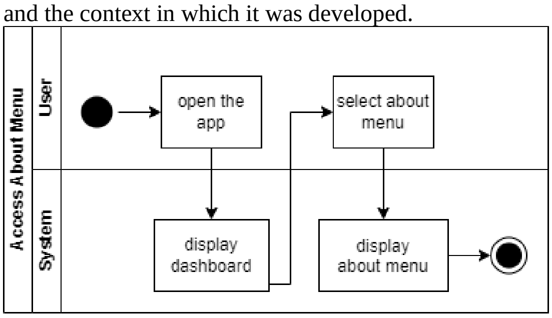

Figure 11: Accessing About Menu Activity

4. RESULT AND DISCUSSION

This chapter presents the comprehensive research process and the outcomes achieved through the development of a mobile-based learning application for the Cipher Feedback (CFB) algorithm. The application integrates various educational components, including learning materials, simulations of the encryption and decryption processes, quizzes for knowledge assessment, and functionalities for performing these cryptographic operations.

4.1 Implementation

Following the completion of the interface design, the implementation phase involved translating the visual elements and user interaction functions into executable program code. This step required meticulous coding practices to ensure that all features operated as intended and that the user interface delivered a smooth and intuitive experience.

To achieve this, a systematic approach was adopted, incorporating user feedback throughout the development process. The application was rigorously tested to validate its functionality and usability before being released to end users. This testing included both automated and manual methods, focusing on ensuring that all components worked seamlessly together.

4.1.1 Main Utama Page

The main menu serves as the homepage of the application, featuring a welcome message and options for navigation. Users can choose from several options, including access to materials, simulations, quizzes, or programs. Figure 12 illustrates the layout of the main menu.

Figure 12: Main Menu Page

4.1.2 Materials Menu Page

The materials menu provides users with access to various content related to the Cipher Feedback (CFB) algorithm. This includes foundational information on CFB concepts, as well as encryption and decryption processes, accompanied by example questions. Figure 13 depicts the structured design of the Materials menu.

Figure 13: Materials Menu Page

4.1.3 Simulation Menu Page

The simulation menu offers users an interactive exploration of the encryption and decryption processes involved in the CFB algorithm. This section enhances user understanding through clear visualizations at each step, effectively illustrating the mechanics of CFB encryption and decryption. Figure 14 showcases the interface design of the Simulation menu, highlighting its educational value.

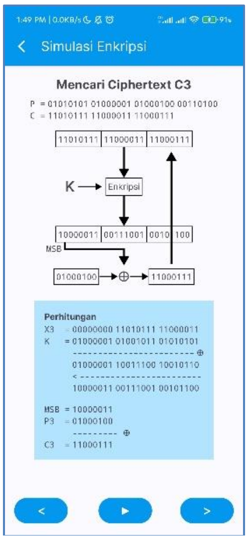

Figure 14: Simulation Menu Page

4.1.4 Quiz Menu Page

The Quiz menu provides a platform for users to assess their understanding of the Cipher Feedback algorithm through a series of multiple-choice questions. These questions cover a range of CFB concepts and offer detailed feedback upon completion. Figure 15 illustrates the interface design of the Quiz menu, demonstrating its role in promoting interactive learning.

Figure 15: Quiz Menu Page

4.1.5 Program Menu Page

In the Program menu, users can seamlessly perform encryption by transforming plaintext into ciphertext using specified key characters, as well as initiate decryption by entering the correct key characters to revert ciphertext back to plaintext. The interface, depicted in Figure 16, is designed to be user-friendly, ensuring that these cryptographic operations can be executed securely and efficiently.

Figure 16: Program Menu Page

4.1.6 Help Menu Page

The Help menu is an essential component of the application, designed to enhance user experience by providing visual aids and textual explanations that facilitate navigation and understanding of the app's functionalities. By incorporating informative images alongside concise and clear text, this menu ensures that users can efficiently explore and utilize the diverse features available within the application, reducing any potential confusion or barriers to effective learning. Figure 17 illustrates the structured visual help in the Guide menu, providing a well-organized framework that assists users in navigating the application and optimizing their learning experience in cryptography..

Figure 17: Help Menu Page

4.1.7 About Menu Page

The About menu provides users with detailed information about the application and the development team. It includes a comprehensive description of the application, a list of key features, developer profiles, the purpose behind the application's development, and acknowledgments to contributors. By presenting this information clearly, users gain a thorough understanding of the application's objectives and benefits. Figure 18 displays the layout of the About menu.

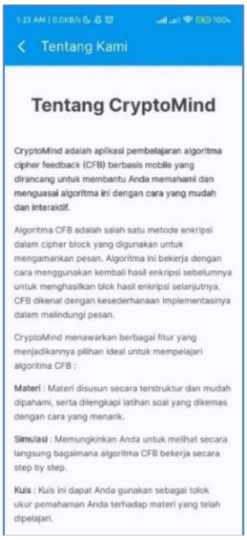

Figure 18: About Menu Page

4.2 Testing

Following the implementation phase, a series of comprehensive tests were conducted to ensure the smooth operation of the learning application while minimizing errors. These tests validated core functionalities and identified potential issues that could affect overall performance. The testing process included various methodologies such as black box testing, System Usability Scale (SUS) testing, and rigorous performance and security evaluations. This systematic approach was crucial for ensuring a seamless user experience aligned with the educational goals of the application.

4.2.1 Black Box Testing

Black box testing focuses on evaluating the software's input and output without analyzing its internal code [22]. This method employed techniques such as Boundary Value Analysis, Equivalence Partitioning, and Decision Table-Based Testing [23]. Conducted under the supervision of Ir. Nur Rochmah Dyah Puji Astuti, S.T., M.Kom., a cryptography lecturer, the testing involved downloading and assessing the Cipher Feedback learning application. Detailed outcomes from this testing are presented in Table 1, showcasing the application's robust performance across various scenarios.

Table 1. Black Box Testing

No	Testing	Result
1	Running the installation process, starting with tapping the APK file or accessing it via a file manager.	valid
2	The application runs well on mobile devices.	valid
3	Displaying the home page as user access navigation to application functionalities and features.	valid
4	The presented materials are appropriate and describe the basic concepts of the Cipher Feedback algorithm.	valid
5	Displaying the simulation page and allowing users to view encryption and decryption visualizations.	valid
6	Displaying the quiz page and allowing users to complete available multiple-choice questions.	valid
7	Displaying results page after users complete the quiz.	valid
8	Displaying the program page and allowing users to enter text for encryption or decryption.	valid
9	Displaying encryption or decryption results based on user input.	valid
10	Ensuring smooth navigation between menus without errors.	valid
11	Ensuring the application can handle invalid inputs without crashing.	valid

4.2.2 Systen Usability Scale

The System Usability Scale (SUS) provides a quick and reliable measure of user experience [24]. Participants in the SUS test included cryptography and computer science students. Due to the small sample size, the SUS is particularly suitable as it delivers accurate usability measurements quickly [25]. Simple random sampling was employed to ensure each participant had an equal chance of selection. Table 2 presents the SUS testing questionnaire

Table 1. System Usability Scale

No.	Testing	Score
1	I think I would like to use this system again.	1-5
2	I found the system unnecessarily complex.	1-5
3	I thought the system was easy to use.	1-5
4	I needed the help of a technical person to use this system.	1-5
5	I thought the features of this system were well integrated.	1-5
6	I found there to be too much inconsistency in this system.	1-5
7	I would imagine that most people would learn to use this system very quickly.	1-5
8	I found the system very cumbersome to use.	1-5
9	I felt very confident using the system.	1-5
10	I needed to learn a lot of things before I could get going with this system.	1-5

5. CONCLUSION

This research presents the development of a mobile-based application designed as a learning tool for the Cipher Feedback (CFB) algorithm, utilizing the Waterfall method. The application aims to enhance the learning experience for students and the general public interested in cryptography.

Testing conducted using the Black Box method confirmed that the application achieved 100% functionality, while the System Usability Scale (SUS) testing also yielded a perfect score, demonstrating the application's effectiveness and usability.

Despite these positive results, the research acknowledges certain limitations, notably that the current simulation only encompasses a single cryptography algorithm. Future development is anticipated to expand the application's capabilities by incorporating dynamic simulations, including additional cryptographic algorithms, and creating an iOS version to complement the existing Android application. This expansion will enhance the overall educational value and accessibility of the application, catering to a wider audience in the field of cryptography.

6. REFERENCES

[1] S. Sadya, ‘Pengguna Smartphone Indonesia Terbesar Keempat Dunia pada 2022’. Available: https://dataindonesia.id/digital/detail/pengguna-smartphone-indonesia-terbesar-keempat-dunia-pada-2022

[2] R. Mustajab, ‘8 Negara dengan Unduhan Aplikasi Terbanyak 2022, Ada Indonesia’ Jul. 22, 2024. Available: https://dataindonesia.id/internet/detail/8-negara-dengan-unduhan-aplikasi-terbanyak-2022-ada-indonesia.

[3] R. Mustajab, ‘Durasi Bermain Aplikasi Mobile di Indonesia Meningkat pada 2022’ Jul. 22, 2023. [Online]. Available: https://dataindonesia.id/digital/detail/durasi-bermain-aplikasi-mobile-di-indonesia-meningkat-pada-2022

[4] D. H. Jayani, ‘Pencurian Data Pribadi Makin Marak Kala Pandemi’, databoks.katadata.co.id. [Online]. Available: https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi

[5] M. Awad, M. Ali, M. Takruri, and S. Ismail, ‘Security vulnerabilities related to web-based data’, *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 2, pp. 852–856, 2019, doi: 10.12928/Telkomnika.v17i2.10484.

[6] P. Kriptografi and I. Rinaldi Munir, ‘Pengantar Kriptografi’, 2004.

[7] R. Umar, A. Yudhana, and A. Dahlan, ‘Analisis Sistem Keamanan Teknik Kriptografi dan Steganografi pada Citra Digital (Bitmap)’, 2019.

[8] I. Riadi, A. Fadil, and F. A. Tsani, ‘Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher’.

[9] S. A. Widiana and I. Firdaus, ‘Implementasi Enkripsi untuk Keamanan SMS Menggunakan Metode Cipher Feedback (CFB) 8-Bit Berbasis Android’, *Journal of Informatics and Computing*, vol. 2, no. 1, pp. 39–47, 2023.

[10] Ayushi, ‘A Symmetric Key Cryptographic Algorithm’, *Int J Comput Appl*, 2010.

[11] H. Hendy and H. Akbar, ‘Pengembangan Aplikasi Android Belajar Kriptografi Sebagai Media Pembelajaran Mata Kuliah Kriptografi’, *Jurnal Informatika*, vol. 8, no. 1, pp. 17–25, 2021, doi: 10.31294/ji.v8i1.9420.

[12] H. D. Hutahaean and P. M. Hasugian, ‘Aplikasi Pembelajaran Kriptograpi berbasis Mobile menggunakan Computer Assisted Instruction’, *Media Informasi Analisa dan Sistem*, vol. 4, no. 1, pp. 1–4, 2019, doi: 10.54367/means.v4i1.310.

[13] S. Hajar, ‘Perancangan Perangkat Lunak Pembelajaran Pemahaman Algoritma Electronic Code Book Menggunakan Metode Computer Assisted Instruction’, *Kakifikom*, vol. 01, pp. 14–22, 2019, [Online]. Available: https://core.ac.uk/download/pdf/287200775.pdf

[14] S. Budidarma, J. Sisingamangaraja, N. 338 Simpang, and L. Medan, ‘Perancangan Aplikasi Pembelajaran Kriptografi pada Algoritma Data Encryption System (DES) Menggunakan Metode Computer Assisted Instruction oleh Riska Oktaria’, *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 2, 2019, [Online]. Available: www.stmik-budidarma.ac.id//

[15] M. F. Dalimuthe, ‘Perancangan Aplikasi Pengamanan File Dokumen Teks Dengan Menggunakan Algoritma Cipher Feedback’, *Jurnal Teknik Informatika UNIKA Santo Thomas*, vol. 04, pp. 70–75, 2019, [Online].

[16] S. Saleh, S. Pd, and M. Pd, ‘Analisis Data Kualitatif’.

[17] M. Badrul, ‘Penerapan Metode Waterfall Untuk Perancangan Sistem Informasi Inventory Pada Toko Keramik Bintang Terang’, vol. 8, no. 2, 2021.

[18] M. Alda, I. Saputri, H. Kurniawan Matanari, and F. Mahmudah, ‘Perancangan Aplikasi Media Pembelajaran TIK Menggunakan Metode Waterfall Berbasis Mobile’.

[19] A. Abdul Wahid Sekolah Tinggi Manajemen Informatika dan Komputer Sumedang, ‘Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi’. [Online]. Available: https://www.researchgate.net/publication/346397070

[20] S. M. Anouncia, M. Cherian, A. Parija, and D. S. R. D. Jayaprasanna, ‘A Framework for Software Architecture Visualization and Evaluation’.

[21] Z. Tuasamu *et al.*, ‘Analisis Sistem Informasi Akuntansi Siklus Pendapatan Menggunakan DFD Dan Flowchart Pada Bisnis Porobico’, 2023.

[22] Rony Setiawan, ‘Black Box Testing Untuk Menguji Perangkat Lunak’, dicoding.com. Accessed: Jun. 20, 2024. Available: https://www.dicoding.com/blog/black-box-testing/

[23] H. Bhasin, E. Khanna, M. Tech Scholar, and P. Sudha, ‘Black Box Testing based on Requirement Analysis and Design Specifications’, 2014.

[24] M. Alvian Kosim, S. Restu Aji, and M. Darwis, ‘Pengujian Usability Aplikasi PeduliLindungi Dengan Metode System Usability Scale (SUS)’, *Jurnal Sistem Informasi dan Sains Teknologi*, vol. 4, no. 2, 2022.

[25] F. Assiri, R. Alshanbari, E. Algamdi, A. Alahmadi, A. Aljehani, and R. Alahmari, ‘Congenital Heart Defect Monitoring System for Children using Internet of Things’, 2017.