eISSN No. : 2976-2278

UTM Computing Proceedings
Innovations in Computing Technology and Applications
Volume: 6 | Year: 2024 | ISBN No. : 2976-2278

Mini-AES Algorithm Visualization for Cryptography Teaching and Learning

Hanis Zainudin and Rashidah Kadir
Faculty of Computing
Universiti Teknologi Malaysia (UTM)
81310 Johor Bahru, Johor, Malaysia
zhanis3@graduate.utm.my, rashidah@utm.my

***Abstract*— This report introduces the Cryptographic Algorithm Visualization System (CAES), designed to enhance students' understanding of cryptographic principles, particularly the Advanced Encryption Standard (AES) algorithm. CAES addresses the challenge of comprehending cryptographic algorithms and aims to promote active learning and engagement. It utilizes visualization techniques and an Agile methodology to offer an intuitive and user-friendly platform for learning AES. CAES also serves as a valuable teaching aid for educators. Overall, this paper presents CAES as a catalyst for improved AES comprehension, knowledge retention, and advancement in information security education.**

Keywords*— *Cryptographic Algorithm Visualization System, AES algorithm, Active learning, Information security education

I. INTRODUCTION

With the growing significance of information technology in our daily lives, the need for comprehensive education in this field has become vital. Cybersecurity, particularly cryptography, plays a crucial role in safeguarding digital information and infrastructure.

Traditional methods of teaching cryptography rely on static resources, leading to passive learning and limited engagement. To address this, the Cryptographic Algorithm Visualization System (CAES) intends to create an interactive platform featuring step-by-step visualizations of cryptographic processes. This encompassed improving students' understanding, fostering higher-order thinking skills, and offering educators a valuable teaching aid.

The scopes include developing an online educational platform with interactive Mini-AES algorithm visualizations, implementing an assessment system, and creating supporting resources for educators. CAES revolutionizes cryptography education by providing dynamic visualizations that bridge the gap between theory and practice, making learning more engaging and effective. It prepare students for careers in cybersecurity and fortifies the digital landscape against evolving threats.

CAES aims to represent a significant advancement in cryptography education, offering students and educators powerful tools to navigate the digital age successfully. In addition, to transform the educational landscape, equipping learners with essential skills while enhancing the overall security of our digital world.

II. LITERATURE REVIEW

This section delves into the fundamental principles of cryptography, visualization, and AES, aiming to achieve a deeper understanding through examples and explanations. The exploration identifies the most suitable tools, methodologies, and technologies for integration into the project.

Within the realm of cryptography education, two distinct approaches exist: traditional and active learning. The traditional method relies on conventional resources like lecture notes and slides, often resulting in passive learning. Active learning, on the other hand, engages students in discussions and collaborative exercises, promoting critical thinking and higher-order cognitive skills.

The Cryptographic Algorithm Visualization System (CAES) prioritizes student-centric learning by immersing students in profound learning experiences. Through interactive components and dynamic visualization tools, CAES revolutionizes how students engage with cryptographic concepts, creating a more engaging and efficient learning environment. This case study showcases the transformative potential of active learning methods, as exemplified by CAES, in higher education, ultimately enhancing the quality and impact of cryptography education.

A. Current Approaches

In the current approaches analysis, UTM employs various methods and approaches for teaching cryptography in its classes. At that time, conventional learning methods were predominant. These methods included classroom lectures supplemented with resources like videos and notes. Students typically studied these materials and then completed paper-based exercises, often lacking confidence in the accuracy of

their solutions. Despite recognizing visualization as a potent learning tool, the traditional approach in cryptography education did not effectively incorporate it, resulting in a shortage of specialized teaching aids.

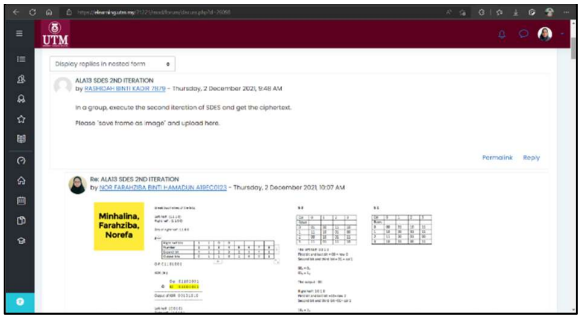

Figure 1 Cryptography Exercises in UTM E-Learning

Figure 1 illustrates the paper-based cryptography exercises submitted by students on the e-learning platform, representing a one-way learning process. Lecturers faced challenges in assessing all student responses in real-time, thus denying students immediate feedback and progress tracking.

Additionally, UTM implements active learning methods to engage students in the learning process, promote critical thinking, and enhance their understanding. While these methods encourage active participation and the development of higher-order thinking skills, they often lack visual aids or interactive tools. This absence of visualizations hindered complete comprehension and the practical application of complex subjects like cryptography, even though active learning methods fostered theoretical comprehension.

.

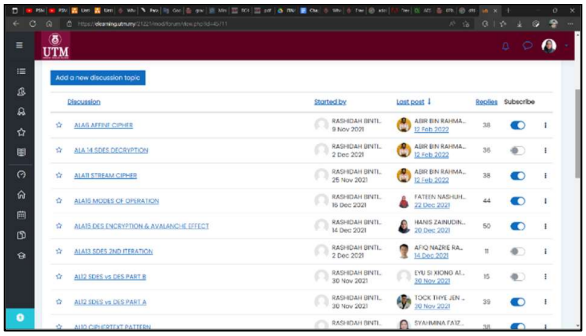

Figure 2 Cryptography Discussions in UTM E-Learning

Figure 2 showcases online discussions within e-learning forums that encourage student engagement. Lecturers will post cryptography-related topics, and students discuss these subjects with one another. However, this method primarily supports theoretical comprehension and aids students mainly in exam performance.

UTM's teaching and learning approaches for cryptography at that time relied heavily on conventional methods and active learning. The former lacks effective visualization tools, while the latter, although promoting critical thinking, still lacks the real-time and tangible aspects that visualizations provide for a comprehensive understanding of cryptography.

B. *Existing Systems*

Next is the exploration of the existing systems related to cryptography education, focusing on their relevance and potential for enhancement. These systems aimed to facilitate learning and understanding of cryptographic concepts, albeit with varying degrees of effectiveness.

1) CrypTool 1: One such system is CrypTool 1, an open-source software widely used for cryptography education and analysis [2]. While valuable, CrypTool 1 had limitations in terms of user-friendliness and modernization, highlighting the need for more intuitive and contemporary educational platforms like the proposed Cryptographic Algorithm Visualization System (CAES).

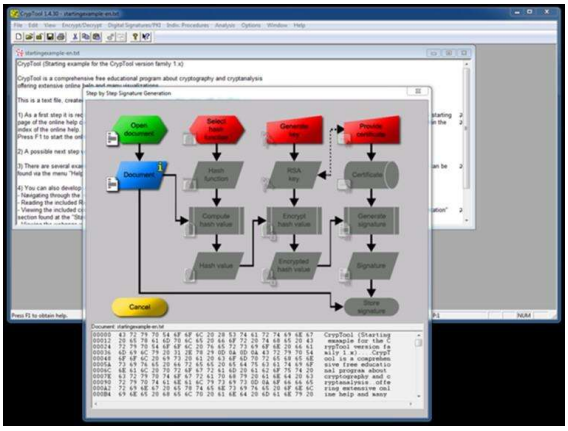

Figure 3 Cryptool 1 Step by Step Execution

In Figure 2.3, the CrypTool 1 Step by Step Signature Generation Execution was showcased. This feature allowed users to gain a comprehensive understanding of how digital signatures are generated, step by step.

2) RC4 Algorithm Visualization: Another system, the RC4 Algorithm Visualization, was designed exclusively for the RC4 symmetric stream cypher algorithm [7]. It provided a step-by-step visual representation of how RC4 functions, assisting users in understanding its inner workings. Such visualizations were critical in improving learning and understanding.o change the default, adjust the template as follows.

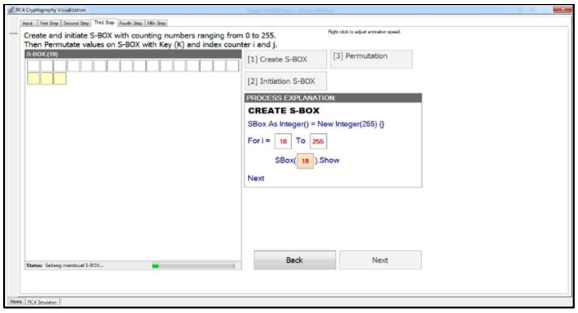

Figure 4 S-Box Table of RC4

Figure 4 shows the development of the S-Box table and its initialization. The process requires building an array with values ranging from 0 to 255, which are then changed during key scheduling [7]. The key scheduling mechanism uses user-supplied keys to initialize the S-Box table, generating cryptographic complexity. Insights from the RC4 Algorithm Visualization System inspired the project, where such an approach benefits in understanding this process, increasing user engagement, and improving the learning of cryptographic principles.

3) GRACE: By offering dynamic visualisation of cryptographic methods, the GRACE (Graphical and Animated Representation for Cryptography teaching) tool redefined cryptographic teaching [2]. These visualisations make complicated processes more accessible and stimulating by streamlining them. GRACE bridges the gap between theory and practise in the field of cryptography education, supporting both instructors and students.o change the default, adjust the template as follows.

Overall, current systems highlight the significance of visualisation in cryptography teaching and influenced the initial development of CAES. The revised CAES intends to expand on this notion by offering a more effective and user-friendly platform for studying and teaching cryptography.

C. Utilized Technologies

This paper continues explores the integration of modern technology tools, with a particular focus on the role of FlutterFlow in educational system development. It highlights how technology has been harnessed to enhance learning experiences, emphasizing the contributions of platforms like FlutterFlow to the evolution of educational technology.

1) Visualizations: The importance of visualization in improving the learning process is emphasized in this study. Charts, diagrams, animations, and interactive interfaces have been found to be consistently beneficial in simplifying complex information, enabling greater learning and increasing knowledge retention. Unlike simulation, visualization uses static or dynamic graphics to convey information in a clear and understandable way, appealing to a variety of learning styles. Visualization appears as a useful technique in the context of cryptographic education, where abstract and sophisticated concepts are used, to break down complex procedures and develop practical.

2) FlutterFlow: FlutterFlow, a developing technology, stands out for its efficiency in the development of online and mobile applications. It provides a visual development paradigm for coordinating user interface design and the production of interactive functions. FlutterFlow's versatility, accessibility, and simplicity make it an effective tool for creating dynamic visual representations in educational environments. Its drag-and-drop interface makes interactive features easier to integrate, boosting the accessibility and engagement of instructional information. Furthermore, its cross-platform features provide greater accessibility across numerous platforms, which is ideal for an effective visualization-based instructional tool. o change the default, adjust the template as follows.

III. IMPLEMENTATION

The implementation of the initial version of the visualization system is discussed. During the implementation phase, the system is deployed on the network to ensure easy access, and it is hosted to make it accessible to users. In the testing phase, users provide feedback on system functionality, usability and overall performance. Their insights play an important role in refining the system for further improvements. The interface of the main functions of the system is displayed in this section, providing a visual representation of the core functions and user interaction.

A. User Authentication

The CAES system's authentication service facilitates user tracking, ensuring secure access through name and password registration. Distinct login procedures are in place for users and administrators, tailored to their roles, ensuring proper access control and role-based functionalities. During implementation, these mechanisms are successfully integrated, contributing to efficient and user-friendly login processes.

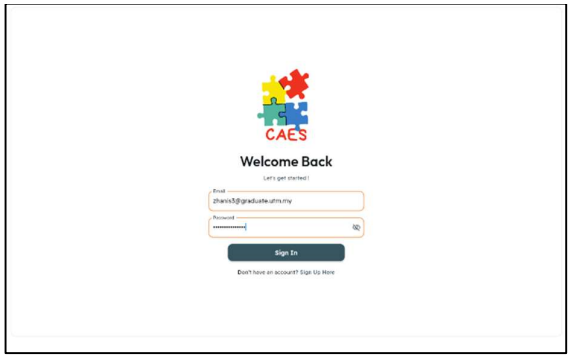

Figure 5 User Authentication

Figure 5 presents the CAES system's authentication page, a crucial element for existing users. This page acts as the gateway to access the system's features. Users are required to input their university email or registered name and a concealed password for security. After entering their credentials and clicking the "Sign In" button, the system verifies the user's information in real-time. Upon successful authentication, users are promptly directed to the system's home page, where they can explore its functionalities and resources. The authentication page functions as a secure checkpoint, ensuring that only authorized individuals access the educational tools and content, prioritizing user data security and system integrity while providing a user-friendly experience.

B. Tutorial Page

Accessible to all users, the tutorial page aids students in studying Mini-AES visualization and serves as a teaching aid for lecturers, despite challenges faced in implementing interactive visualizations as initially intended.

C. *Quizzes Page*

Accessible to all users, this page offers randomly generated quizzes, promoting active learning and engagement with cryptographic concepts. Users can track progress and view marks, receiving valuable feedback on their performance.

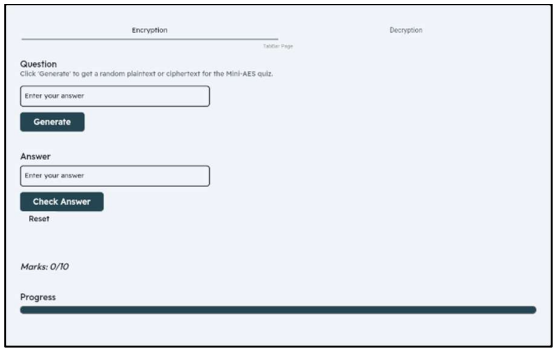

Figure 6 Quizzes Page of CAES System

Figure 6 illustrates the Quizzes Page, a dynamic feature in the CAES system designed to reinforce users' understanding of the Mini-AES algorithm. Users can test their knowledge and problem-solving skills with randomly generated plaintext or ciphertext. Immediate feedback indicates the correctness of their responses. Users can also access step-by-step visualizations to review algorithmic processes, promoting active learning and concept retention. This feature aligns with the CAES system's goal of enhancing cryptography education through interactive and practical application.

D. *Notes Page*

Dedicated to Mini-AES notes and educational resources, this section enhances students' theoretical understanding. Lecturers can upload supplementary materials, supporting students' academic progress.

E. *Admin Dashboard*

Serving as the central command center for administrators, this dashboard provides insights into system updates, report generation, and user management, optimizing system performance and user satisfaction.

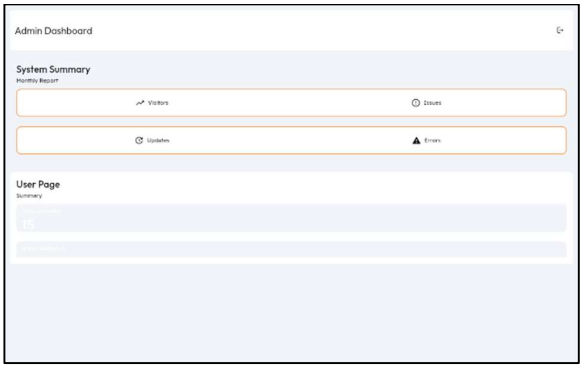

Figure 7 Admin Dashboard

Figure 7 presents the Admin Dashboard, an exclusive control center within the CAES system for authorized administrators. To access it, administrators must log in with their credentials. The Admin Dashboard offers a comprehensive view of the system's performance, displaying visitor statistics and real-time monitoring of system health. It also provides updates and reporting features. With its user-friendly interface, administrators can efficiently manage and monitor the CAES system, ensuring optimal operation and user satisfaction.

IV. DISCUSSIONS

The project is partially successful in developing and deploying a platform for education that incorporates interactive visualization into cryptography instruction. This accomplishment broadens learning opportunities for students and instructors, encouraging a greater comprehension of complicated cryptographic principles. The system's functionality enables users to access the online platform, authenticate themselves, access learning resources, track progress, and operate the system efficiently. This feature simplifies the educational process and boosts user engagement. User authentication has been prioritized to maintain security and privacy, both of which are key components of educational platforms.

Although this project encountered various obstacles such as resource limits and a lack of experience in visualization implementation, major impediments were formed. Time restrictions and tool compatibility constraints burden the process even further. Due to these limitations, the fundamental goal of establishing an interactive platform with dynamic visualization was not completely realized. Although this project encountered various obstacles such as resource limits and a lack of experience in visualization implementation, major impediments were formed. Time restrictions and tool compatibility constraints burden the process even further. Due to these limitations, the fundamental goal of establishing an interactive platform with dynamic visualization was not completely realized.

Insights acquired recommend picking initiatives that correspond with existing resources and putting together focused teams with various abilities for future improvements. An in-depth review is recommended before prioritizing the suitable tools for the project's duration and complexity. Furthermore, ongoing enhancements such as expanding the visualization collection, enhancing the user interface, and incorporating user feedback mechanisms might result in a more comprehensive and user-friendly instructional platform. Addressing these issues and making improvements will lead to more substantial outcomes for projects in the future.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to Faculty of Computing and Universiti Teknologi Malaysia (UTM) for their invaluable support and resources, which played a crucial role in the successful research.

REFERENCES

[1] Cattaneo, G., De Santis, A., & Ferraro Petrillo, U. (2008). Visualization of cryptographic protocols with GRACE. *Journal of Visual Languages & Computing, 19*(2), 258-290.

[2] Ma, Jun & Tao, Jun & Mayo, Jean & Shene, Ching-Kuang & Keranen, Melissa & Wang, Chaoli. (2016). *AESvisual: A visualization tool for the AES cipher*. 230-235.

[3] Piotr Olczak. (2022, March 30). *Data visualizations for schools.* The International Educator (TIE Online).

[4] Pithadiya, K. (2023, July 31). *What is FlutterFlow?* Scaler Topics.

[5] Simms, Xavier. (2011). *Enhancing cryptography education via visualization tools.* Proceedings of the Annual Southeast Conference. 344-345.

[6] Sriadhi, S., Rahim, R., & Ahmar, A. S. (2018). *RC4 Algorithm Visualization for Cryptography Education*. Journal of Physics: Conference Series, 1028, 012057.

[7] *Teaching students to use visualization to improve comprehension*. (n.d.). Education World | Connecting educators to what works.

[8] The Sage Development Team. (n.d.). *Mini-AES - Cryptography*. SageMath Documentation.

[9] *What is FlutterFlow?* A comprehensive guide, review, and exploration of alternatives. (2023, September 14). Low Code Agency - No-Code Development Agency.

[10] Xavier Simms and Hongmei Chi. 2011. Enhancing cryptography education via visualization tools. In Proceedings of the 49th Annual Southeast Regional Conference (ACM-SE '11). Association for Computing Machinery, New York, NY, USA, 344–345.