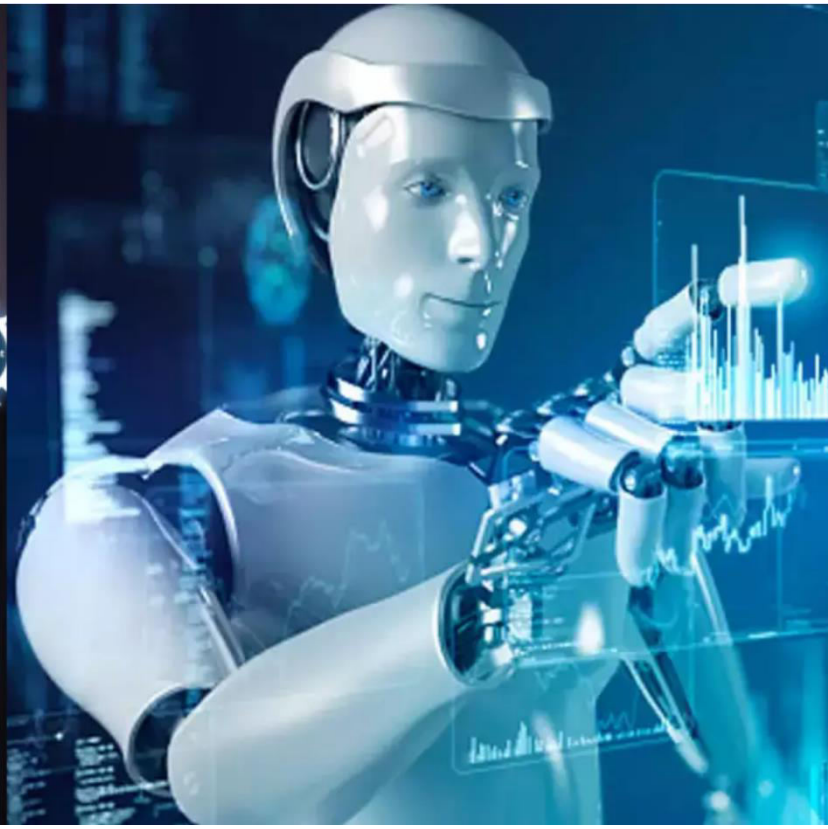
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 6, June 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406207|

CipherCraft Pro: A Secure Symmetric Encryption Toolkit Detection

Anisha Rajendra Patil[1], Dr. Madhavi Kishor Chaudhari [2], Dr. Manisha Bharati[3]

M.Tech (Information Security) Student, Department of Technology, Savitribai Phule Pune University, Pune, India[1]

Assistant Professor, Department of Technology, Savitribai Phule Pune University, Pune, India[2]

Associate Professor, Department of Technology, Savitribai Phule Pune University, Pune, India[3]

ABSTRACT: The system presents the design and development of a web-based application aimed at demonstrating secure symmetric encryption and decryption techniques. The primary goal is to create an intuitive and interactive platform to aid in the educational understanding of cryptographic principles. CipherCraft Pro focuses on implementing robust features such as authenticated encryption, secure key derivation, and responsive user interaction to simulate real-world cryptographic scenarios.The application integrates an encryption module using the Fernet standard, which combines AES-128 in CBC mode with HMAC-SHA256, ensuring confidentiality and integrity. It also includes a decryption module and comprehensive key management options, including secure Fernet key generation and password-based key derivation using PBKDF2-HMAC-SHA256 with configurable salts and iteration counts. The system's frontend is developed using HTML, Tailwind CSS, and JavaScript to ensure responsiveness and user-friendliness, while the backend is powered by Python and Flask for efficient cryptographic processing.Employing a practice-led, iterative development methodology, the project emphasizes functional correctness, secure implementation, and ease of use. CipherCraft Pro serves as a hands-on learning tool for students and enthusiasts, bridging theoretical cryptography with practical application, and contributing significantly to cybersecurity education through demonstrative visualization of symmetric encryption concepts.

KEYWORDS: Symmetric Encryption, Fernet, AES-CBC, HMAC-SHA256, PBKDF2, Key Derivation, Cryptography, Information Security, Web Application Security, Flask, Python, JavaScript, Tailwind CSS, Educational Software.

I. INTRODUCTION

In today's digitally connected world, securing information through cryptography is not just essential—it's foundational. With growing threats to data privacy and the increasing complexity of cyberattacks, understanding how cryptographic systems work is vital for both professionals and learners in the field of cybersecurity. Among the various cryptographic techniques, symmetric encryption stands out for its efficiency and speed, particularly in environments where performance and resource optimization are critical. Symmetric encryption uses a single secret key for both encryption and decryption processes, making it a cornerstone of many secure communication systems.

The project CipherCraft Pro was born from the need to bridge the gap between theoretical cryptography and practical application. While there are countless tutorials and academic texts explaining symmetric encryption, learners often lack access to hands-on tools that can visually and interactively demonstrate cryptographic operations. At the same time, professional-grade tools are often too complex or opaque for educational use. This project aims to fill that gap by delivering an interactive web-based platform that illustrates key symmetric encryption principles in a way that is clear, practical, and educational.

The core motivation behind CipherCraft Pro is to empower users—especially students, educators, and early-stage developers—with the ability to observe and experiment with secure cryptographic practices in a controlled environment. The platform offers not just functionality but also insight into secure implementation. For instance, it integrates authenticated encryption using the Fernet module, which combines AES-128 in CBC mode with HMAC-SHA256 to provide both confidentiality and data integrity. It also introduces users to secure key management, including the generation of cryptographically secure keys and password-based key derivation using PBKDF2-HMAC-SHA256, incorporating best practices like the use of salts and adjustable iteration counts.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406207|

The application is built with a clean, responsive user interface using HTML, Tailwind CSS, and JavaScript. This interface includes usability features such as password strength indicators and real-time feedback on encryption/decryption processes. The backend, developed with Python and Flask, handles all cryptographic operations securely and efficiently, ensuring a smooth and safe user experience.

The objectives of the project were multi-fold: to implement robust encryption and decryption, to demonstrate secure key management, to build an engaging user interface, to provide educational clarity, and to ensure functional correctness through testing. The project's scope includes the development of text-based encryption and decryption features, user-generated and derived key management, and base64-encoded outputs suitable for learning and experimentation. However, the tool does come with certain limitations. It has not undergone formal security audits, does not support asymmetric cryptography or file encryption, and lacks persistent user authentication or cross-device synchronization.

In conclusion, CipherCraft Pro is not intended for securing high-value production data but rather serves as a secure, functional, and educational platform. By providing practical exposure to symmetric encryption principles, it plays a meaningful role in enhancing cryptographic literacy and promoting secure coding habits among learners and professionals alike.

II. LITERATURE SURVEY

The foundation of CipherCraft Pro is grounded in established cryptographic principles, with a focus on symmetric key encryption. Symmetric encryption employs a single key for both encryption and decryption, offering high computational efficiency and widespread use in data security applications. Among the algorithms, AES (Advanced Encryption Standard) is the preferred choice due to its strength and standardization by NIST. CipherCraft uses Fernet, a high-level API that combines AES-128 in CBC mode with HMAC-SHA256 to ensure confidentiality and integrity.

To address the issue of weak password entropy, PBKDF2 (Password-Based Key Derivation Function 2), as defined in RFC 2898, is employed. This standard applies a pseudorandom function (HMAC-SHA256) to transform user passwords into secure cryptographic keys, using random salts and configurable iteration counts for added protection.

1. **Katz, Lindell (2021)** – Introduction to Modern Cryptography explains fundamental symmetric encryption principles and AEAD concepts.
2. **NIST FIPS PUB 197 (2001)** – Specifies AES as the federal standard for block cipher encryption.
3. **RFC 2898 (Kaliski, 2000)** – Describes PBKDF2 standard used for secure password-based key derivation.
4. **RFC 2104 (Krawczyk et al., 1997)** – Introduces HMAC used in Fernet for authentication.
5. **Cryptography.io Docs** – Provides practical implementation guidance for Fernet encryption.
6. **OWASP Top 10 (2021)** – Lists critical web application security concerns including input validation and secure data handling.
7. **Flask Docs (Pallets Projects)** – Details best practices for secure and scalable Python web API development.
8. **Tailwind CSS Docs (Tailwind Labs)** – UI design framework supporting accessibility and responsive styling.
9. **Jain et al. (2020)** – Reviewed usability factors in cryptographic tools highlighting educational UI needs.
10. **Huang & Stobert (2019)** – Explored usability of encryption interfaces emphasizing feedback and simplification.

Further, secure web application design principles such as input validation, error handling, and HTTPS considerations are incorporated to ensure a safe learning environment. Tailwind CSS enhances the user interface, ensuring clarity and responsiveness crucial for usability in educational cryptographic tools.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406207|

III. METHODOLOGY

CipherCraft Pro follows a **practice-led iterative model** involving planning, secure design, coding, testing, and user-centered refinement.

1) System Architecture

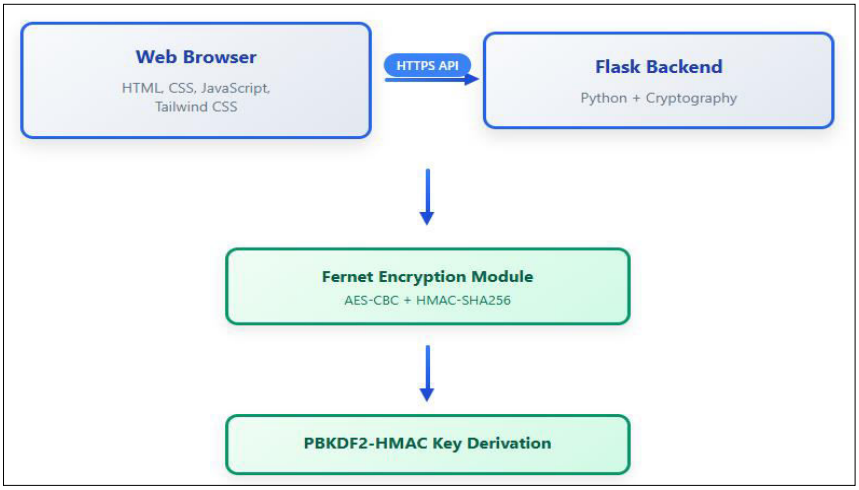


Fig: System Flow

2) Process Steps

1. Requirement Analysis: Defined the aim of developing an educational symmetric encryption toolkit.
2. Technology Stack Selection: Python with Flask for the backend; HTML, Tailwind CSS, and JavaScript for the frontend.
3. Backend Implementation: Focused on symmetric encryption using Fernet and key derivation using PBKDF2.
4. Frontend Development: Designed for user-friendly interaction with features like password strength indicators.
5. Testing and Refinement: Conducted functional and usability testing; refined UI/UX and error messages.

3) Component Explanation

1) **User Interface (UI)**: Built with HTML/CSS and Tailwind for modern, responsive interaction.
2) **Frontend Logic**: JavaScript manages input validation, encryption/decryption commands, and UI updates.
3) **API Layer (Flask)**: Acts as the secure bridge between UI and backend cryptographic functions.
4) **Backend Logic (Python)**: Hosts secure operations like key generation, Fernet encryption, and PBKDF2 derivation.
5) **Fernet Module**: Combines AES-CBC and HMAC-SHA256 ensuring confidentiality + integrity.
6) **PBKDF2-HMAC-SHA256**: Derives cryptographically strong keys from user passwords.
7) **Data Flow**: Processed and returned between layers using Base64 URL-safe format.

IV. EXPERIMENTAL RESULTS

CipherCraft Pro was tested using multiple encryption/decryption workflows:

[1] Functional Results

- Encryption/Decryption: Works flawlessly with auto-generated and password-derived keys.
- Validation: Rejects incorrect salt, key, or iteration combinations and guides users via alerts.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406207|

- Password Strength Meter: Evaluates security in real time to encourage strong practices.
- User Interface: Responsive, intuitive, and visually modern.

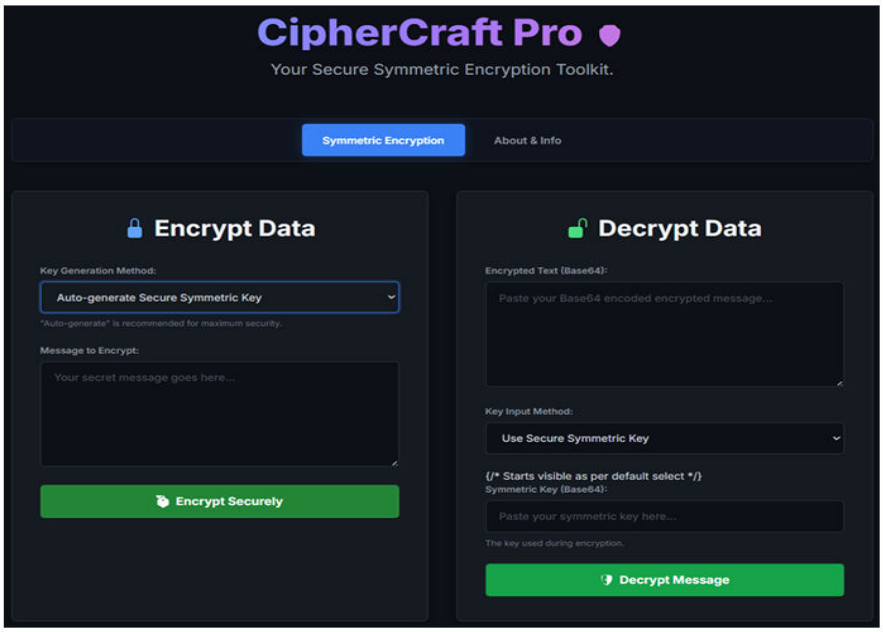


Fig: CipherCraft Pro- Encryption Interface showcasing key method selection and input fields

Fig: CipherCraft Pro- Decryption Interface with options for key input.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406207|

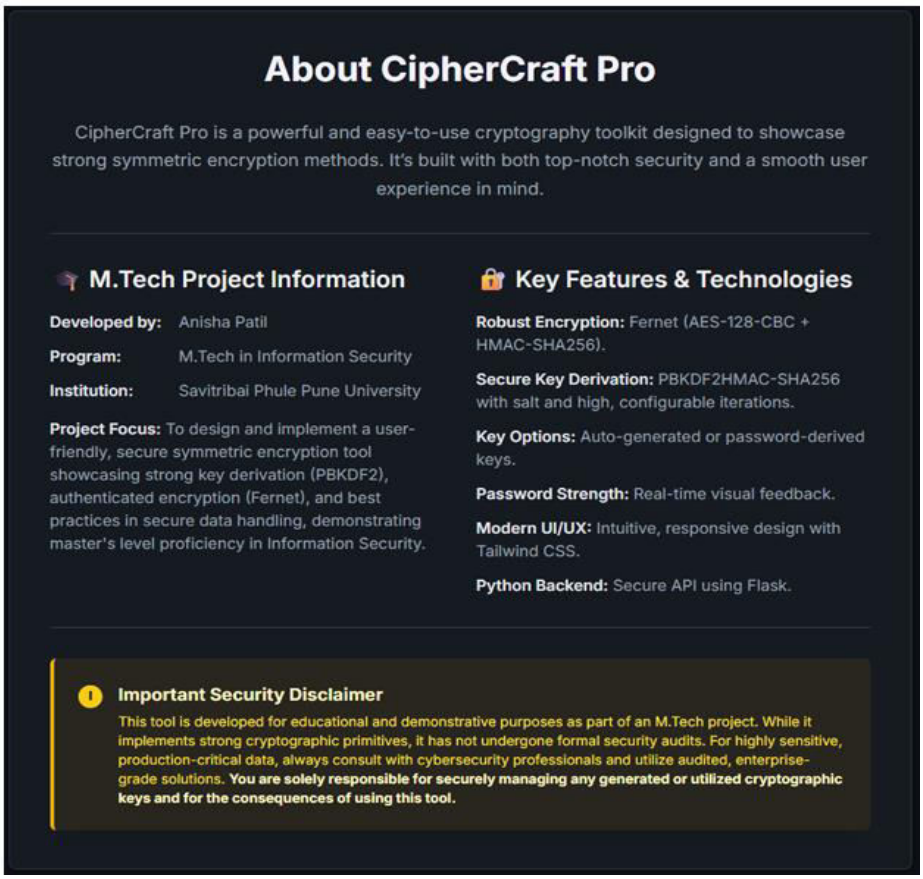


Fig: CipherCraft Pro- "About & Info" section providing project context and disclaimer

V. CONCLUSION

The CipherCraft Pro demonstrates a secure, interactive, and educational approach to symmetric encryption. Designed with a pedagogical focus, it bridges theory and practice through real-time visual interaction. Leveraging Fernet (AES-CBC + HMAC-SHA256) and PBKDF2 for key derivation, the system ensures confidentiality, integrity, and enhanced key management. The responsive web interface simplifies complex cryptographic processes, making them approachable for learners. Backed by a Python Flask API, CipherCraft Pro securely performs cryptographic operations while the frontend provides dynamic feedback and intuitive flow. Iterative testing confirmed the correctness, usability, and robustness of the tool. The system empowers users to explore and understand cryptographic concepts practically, fulfilling its educational mission. With future enhancements such as file encryption, asymmetric cryptography, and persistent key management, CipherCraft Pro holds strong potential to evolve into a comprehensive cryptographic learning platform.k.

REFERENCES

[1] Cryptography.io Developers. (n.d.). Fernet (symmetric encryption). Cryptography.io Documentation. Retrieved [Date Accessed], from https://cryptography.io/en/latest/fernet/
[2] Katz, J., & Lindell, Y. (2021). Introduction to Modern Cryptography (3rd ed.). CRCPress.
[3] National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197: Advanced Encryption Standard (AES).U.S.DepartmentofCommerce.Retrieved[DateAccessed],fromhttps://csrc.nist.gov/publications/detail/fips/197/final

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 6, June 2025

|DOI: 10.15680/IJIRSET.2025.1406207|

[4] National Institute of Standards and Technology (NIST). (2010). Special Publication 800-132: Recommendation for Password-Based Key Deriva tion. U.S. Department of Commerce. Retrieved [Date Accessed], from https://csrc.nist.gov/publications/detail/sp/800-132/final

[5] Open Web Application Security Project (OWASP). (2021). OWASP Top 10- 2021. Retrieved [Date Accessed], from https://owasp.org/Top10/

[6] Krawczyk, H., Bellare, M., & Canetti, R. (1997). RFC 2104: HMAC: Keyed Hashing for Message Authentication. Internet Engineering Task Force. Retrieved [Date Accessed], from https://www.rfc-editor.org/info/rfc2104

[7] Kaliski, B. (2000). RFC 2898: PKCS #5: Password-Based Cryptography Specifi cation Version 2.0. Internet Engineering Task Force. Retrieved [Date Accessed], from https://www.rfc-editor.org/info/rfc2898

[8] Tailwind Labs. (n.d.). Tailwind CSS Documentation. Retrieved [Date Accessed], from https://tailwindcss.com/docs [9] Pallets Projects. (n.d.). Flask Documentation. Retrieved [Date Accessed], from https://flask.palletsprojects.com/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details