BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Autonomous Institute under VTU, Belagavi, Karnataka - 590 018

Yelahanka, Bengaluru, Karnataka - 560064

Information and Network Security (BCS701) CCA Report

On

"CIPHER-DRIVEN LOGIN SYSTEM"

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

by

CHITHRAPRAGATHI K N 1BY23CS405

Under the Guidance of

Prof. Beerappa
Asst. Professor
Dept. of CSE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Avalahalli, Yelahanka, Bengaluru, Karnataka -560064
2025-26

TABLE OF CONTENTS

Content **Page Number**

Abstract

The **Cipher-Driven Login System** is a secure web-based authentication application designed to validate user access using encryption. It allows a user to enter a message, encrypt it using AES (Advanced Encryption Standard), decrypt it again, and then login **only if the decrypted text matches the original message**. This ensures secure verification without storing any passwords or sensitive data.

The system is implemented completely using HTML, CSS, and JavaScript with the CryptoJS AES library for strong encryption. All operations occur within the browser, ensuring data privacy because no information is stored on a server. This lightweight but highly secure design demonstrates the importance of encryption-based authentication and client-side validation in modern security systems.

Introduction

Security in digital applications is essential as authentication systems increasingly face threats such as password leaks, data breaches, and unauthorized access. Traditional login systems rely on stored credentials, which can be compromised if the server is attacked.

To solve these problems, the **Cipher-Driven Login System** uses an **encryption-based login mechanism**, where authentication depends on correctly encrypting and decrypting data. Instead of storing credentials, the system checks whether the decrypted message matches the original message entered by the user. If both match, the user is allowed to access the next page (shopping website).

This provides a secure, efficient, and server-independent authentication mechanism. The system also demonstrates the practical use of symmetric encryption in user validation processes.

Problem Statement

Traditional login systems are vulnerable because:

- User credentials are stored on servers.
- Attackers can steal or guess passwords.
- Password databases can be leaked.
- A server breach exposes all user accounts.

Additionally, many authentication systems do not use strong encryption for verifying user data, making them weaker against attackers.

Hence, there is a need for a **secure, encryption-driven login mechanism** that:

1. Does **not require storing passwords**.
2. Uses **strong client-side encryption**.
3. Validates the user securely without server interaction.
4. Uses a simple and user-friendly interface.

The Cipher-Driven Login System solves these issues by verifying login through AES encryption–decryption matching.

System Requirements

4.1 Hardware Requirements

- Laptop or PC with minimum 4GB RAM
- Processor: Intel i3 or above
- 500 MB free storage
- Browser-supported device (Laptop / Mobile)

4.2 Software Requirements

- HTML, CSS, JavaScript
- CryptoJS (AES Encryption Library)
- Web browser (Chrome, Firefox, Edge)

4.3 Additional Tools

- VS Code or any text editor
- Live Server plugin (optional)

Design and Implementation

5.1 System Architecture Design

The system is divided into three layers:

1. User Interface Layer

- Created using HTML & CSS
- Contains fields for:
    - Enter message
    - Enter password
    - Encrypted text
    - Decrypted text
- Buttons:
    - Encrypt
    - Decrypt
    - Login

2. Application Logic Layer (JavaScript)

- Uses CryptoJS AES encryption.
- Handles:
    - Encryption of message
    - Decryption of encrypted text
    - Login validation

3. Access Control Layer

- Login allowed **only when**:
- `Original Message == Decrypted Message`
- On success → Redirect to shopping website.

5.2 Detailed Workflow

A) Encrypting a Message

1. User enters text and password.
2. System encrypts using AES.
3. Encrypted output is displayed.

B) Decrypting a Message

1. User enters encrypted text and same password.
2. System decrypts it.
3. Decrypted text is displayed.

C) Login Process

1. System compares:
   - Message entered first
   - Decrypted result
2. If they match → redirects user.
3. If not → displays an error.

Security Analysis

The Cipher-Driven Login System provides strong security features:

1. AES Encryption

Uses AES-256 (via CryptoJS) for securing messages.

2. No Server Storage

No passwords or messages are stored anywhere.

3. Replay Attack Protection
Validation requires correct user input each time.

4. Man-in-the-Middle Safety

All operations occur locally inside the browser.

5. Brute-Force Attack Resistance

Strong AES encryption makes guessing passwords difficult.

Test Case	**Input**	**Expected Output**	**Result**
Encrypt message	Text + password	Encrypted string	Pass ✔
Decrypt with correct password	Encrypted text	Original text	Pass ✔
Decrypt with wrong password	Wrong key	Error alert	Pass ✔
Login with matching text	Same text	Redirect	Pass ✔
Login with mismatching text	Different values	Error message	Pass ✔
Empty fields	None	Warning message	Pass ✔

System Testing

Functional Testing

- Verified that users can enter messages and passwords without errors.
- Checked that encryption happens correctly and instantly after clicking the encrypt button.
- Ensured that the decryption function reproduces the exact original message when the correct password is used.
- Confirmed that entering a wrong password results in unreadable or incorrect decrypted text.

Login Validation Testing

- Verified that login succeeds only when the original message and decrypted message are exactly the same.
- Confirmed that the system redirects the user to the shopping website upon correct validation.
- Checked that the system displays an “Access Denied” message when the messages do not match.

Error Handling Testing

- Tested empty input fields and ensured the system displays warnings such as “Enter Message.”
- Checked that login cannot proceed unless encryption and decryption steps are completed.
- Ensured no unexpected behaviour occurs when clicking buttons with incomplete input.

Cross-Browser Compatibility

- Tested on Google Chrome, Mozilla Firefox, and Microsoft Edge.
- Verified that the interface works consistently in all browsers.

Responsiveness Testing

- Confirmed the UI adapts properly to mobile, tablet, and desktop screens.
- Buttons, text boxes, and outputs display correctly across devices.

Security Testing

- Verified that AES encryption protects the message and cannot be reversed without the password.
- Ensured no plaintext message is stored anywhere in the browser’s memory.
- Confirmed resistance to simple brute-force attempts.

Performance Testing

- Checked that encryption and decryption occur within milliseconds.
- Verified that the system handles repeated operations without lag.

Innovation and Application Relevance

1. Message-Based Authentication

Instead of traditional passwords or OTPs, this system verifies identity by confirming whether:

Decrypted text matches the original message.

This introduces a new and creative security check for controlled access.

2. Real-Time AES Encryption in the Browser

- No data sent to serverEverything happens in the client browser (local security)
- Zero risk of data exposure

3. Secure Login Redirection

The user gets access to the shopping website **only if** the encryption-decryption process is correct, ensuring enhanced security.

4. Lightweight Web-Based Design

- No installation required
- Completely browser-driven
- Accessible from any device

5. Error-Proof Validation Logic

The system eliminates incorrect logins using a **dual-check mechanism**:

- Original message
- Decrypted message

Both must match.

8.2 Application Relevance

This system is highly relevant in environments where **privacy, authentication, and secure message exchange** are essential.

1. E-Commerce Security

Used to authenticate users before redirecting to:

- shopping portals
- payment gateways

Innovation and Application Relevance

2. Educational Platforms

Students or faculty can securely access:

- exam portals
- assignment uploads
- student dashboards

Only after AES validation.

3. Corporate Frameworks

Employees can access:

- project dashboards
- internal tools
- attendance systems

With encryption-based authentication.

4. Secure Messaging Demonstration

Ideal for teaching encryption concepts in:

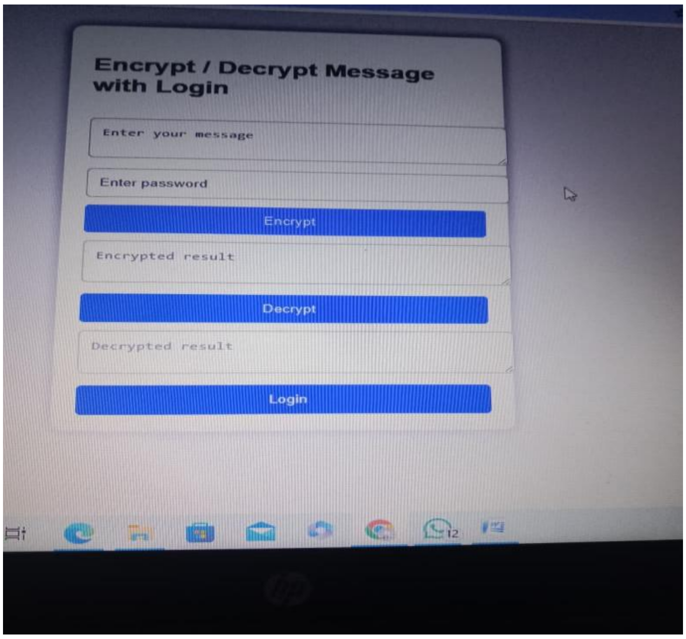
- Computer Science
- Information Security
- Cryptography labs

5. Personal Data Protection

Useful for private communication where:

- only correct users can access content
- AES protects message confidentiality

Outputs



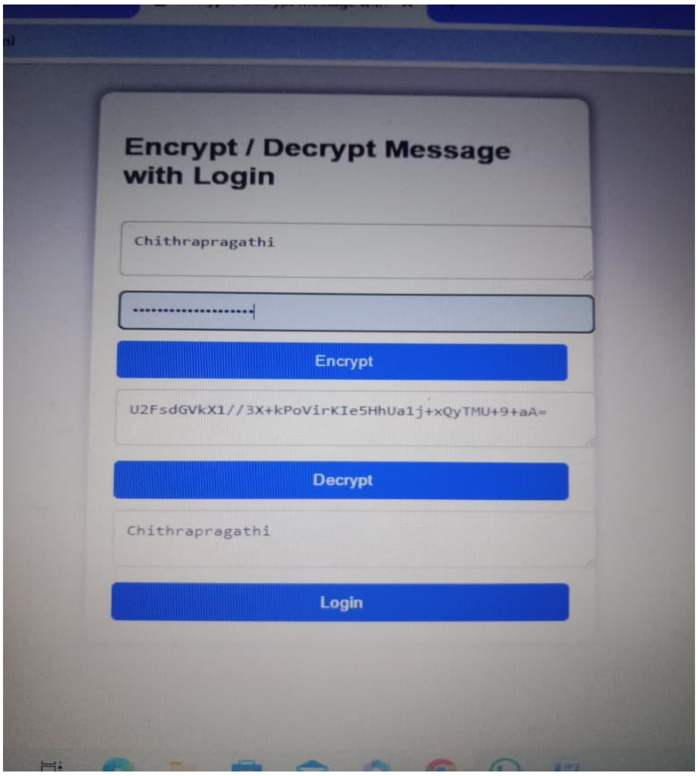
Encrypt / Decrypt Message with Login

Enter your message

Enter password

Encrypted result

Decrypted result



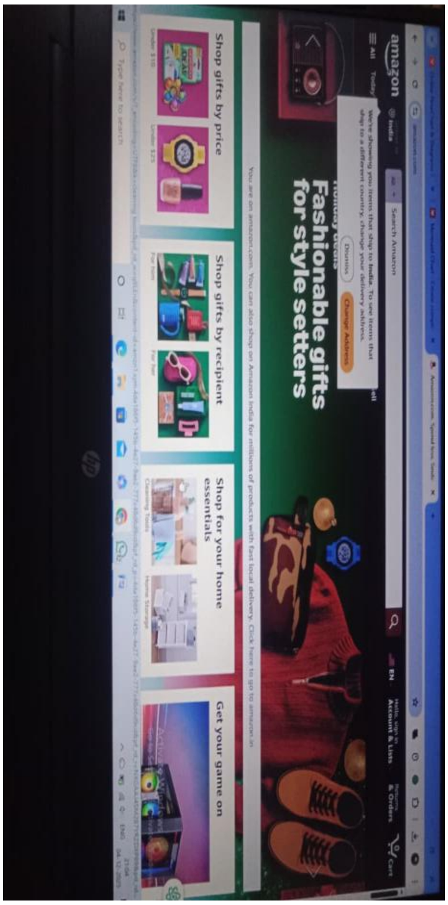
Encrypt / Decrypt Message with Login

Chithrapragathi

•••••••••••••••••••

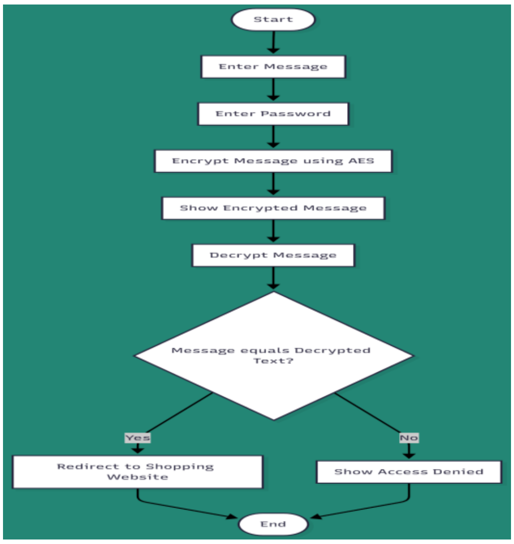
U2FsdGVkX1//3X+kPoVirKIe5HhUa1j+xQyTMU+9+aA=

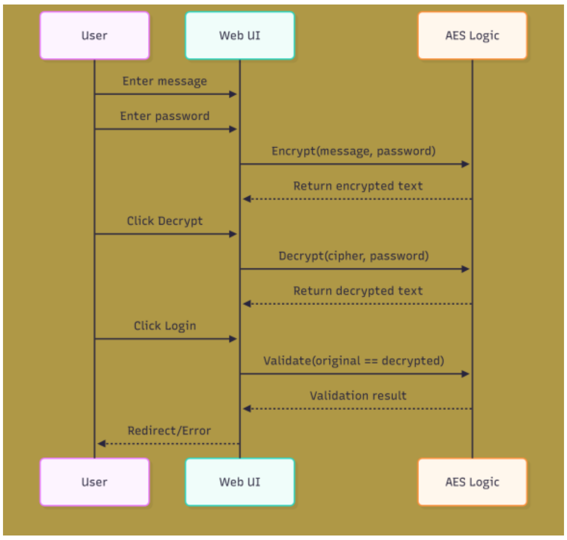
Chithrapragathi

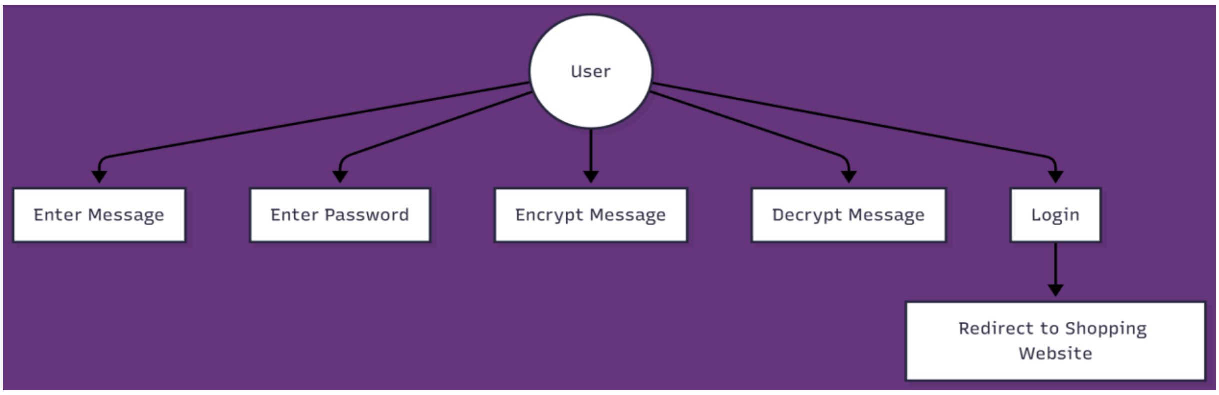


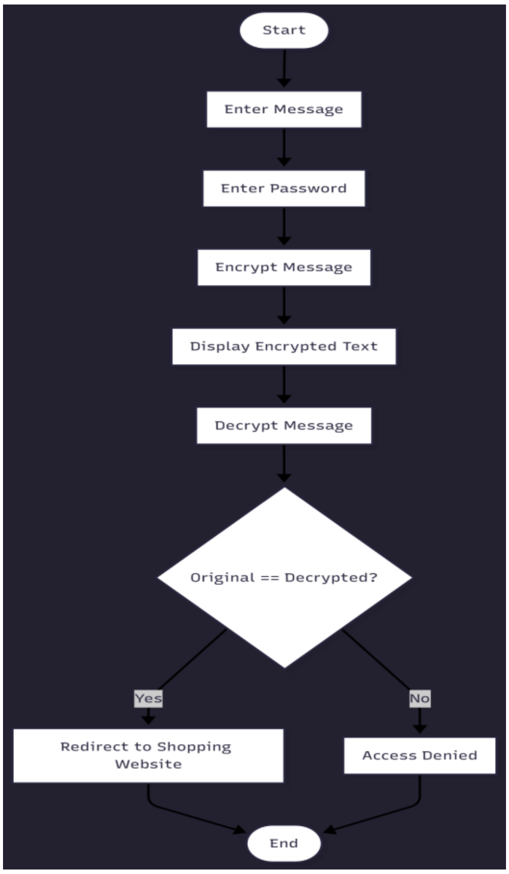
amazon
Fashionable gifts for style setters
Shop gifts by price
Shop gifts by recipient
Shop for your home essentials
Get your game on

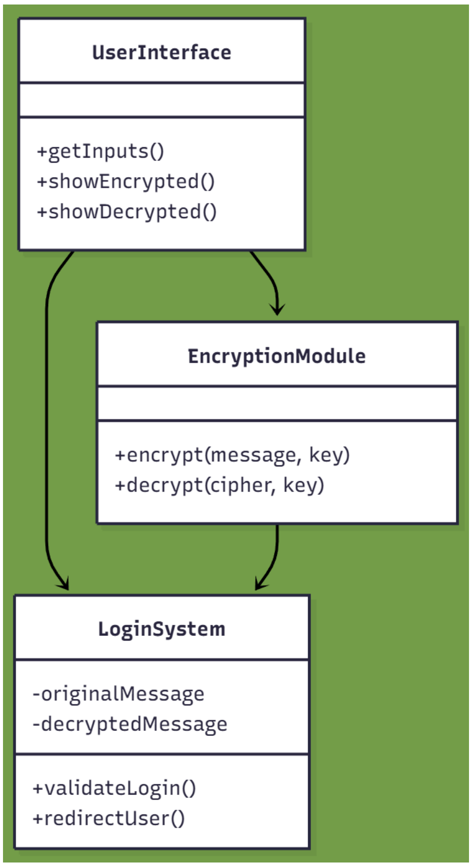
IMPORTANT DIAGRAMS











Conclusion

The Cipher-Driven Login System demonstrates how encryption can be effectively used to validate user authentication without relying on stored passwords. The use of AES encryption ensures high levels of security, while the client-side implementation guarantees complete privacy.

The project is simple, efficient, secure, and highly relevant to modern cybersecurity needs. It can be extended further with database integration, OTP validation, QR-code based encryption, and multi-user support to create a full-scale secure authentication platform.

References

1. CryptoJS Documentation – https://cryptojs.gitbook.io
2. MDN Web Docs – JavaScript & Web APIs
3. OWASP Secure Coding Practices
4. HTML & CSS W3Schools Documentation
5. JavaScript Official Documentation