#### Project report on

**Symmetric Encryption using Mcrypt**

**A Dissertation submitted in partial fulfillment of the Academic requirements for the award of the degree of**

**Bachelor of Technology**

## In

**Computer Science & Engineering (Cyber Security)**

**Submitted by**

Sitale Apurwa (22H51A6249) Tharun Vubbapally (22H51A6254) Pranav Vancha (22H51A6259)

**Under the esteemed Guidance of**

**Dr.R.Venkateswara Reddy (Associate Professor and HOD,CSC)**

**Department of Cyber Security**

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

#### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

**DEPARTMENT OF CYBER SECURITY**



#### CERTIFICATE

This is to certify that the Mini Project -1 report entitled “**Vulnerability Assessment and penetration Testing (VAPT)**” being submitted by **Sitale Apurwa (22H51A6249), Tharun Vubbapally (22H51A6254), Pranav Vancha (22H51A6259)** in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a record of bonafide work carried out his/her under my guidance and supervision.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree.

Dr. Punyaban Patel Dr. R. Venkateswara Reddy

( Professor Associate Professor & HOD

Dept. of CSC ) Dept. of CSC

#### 

#### ACKNOWLEDGEMENT

With great pleasure I want to take this opportunity to express my heartfelt gratitude to all the people

`who helped in making this project a grand success.

I am grateful to **Dr. Punyaban Patel**, Professor, Dept. of Computer Science and Engineering for her valuable suggestions and guidance during the execution of this project.

I would like to thank **Dr. R. Venkateswara Reddy**, Head of the Department of Computer Science and Engineering, for his moral support throughout the period of my study in CMRCET.

I am highly indebted to **Major Dr. V.A. NARAYANA**, Principal CMRCET, for giving permission to carry out this project in a successful and fruitful way.

I would like to thank the Teaching & Non- teaching staff of the Department of Computer Science and Engineering for their co-operation.

Finally, I express my sincere thanks to **Mr. CH. GOPAL REDDY**, Secretary, CMR Group of Institutions, for his continuous care. I sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project work.

Sitale Apurwa (22H51A6249)

Tharun Vubbapally (22H51A6254)

Pranav Vancha (22H51A6259)

#### 

#### ABSTRACT

* In this project, we explore the implementation of symmetric encryption using the MCRYPT command-line tool in the Kali Linux operating system. The project focuses on file encryption and decryption, allowing users to safeguard their files with a passphrase.
* Through the MCRYPT utility, users can encrypt files using a chosen passphrase, generating an encrypted version of the file with the ".nc" extension. Subsequently, decryption of the encrypted file is achieved by providing the correct passphrase, enabling access to the original content.
* It serves as a high-level overview for stakeholders , highlighting the security posture of the tested environment.
* Also the use of java to encrypt the username and password and storing the encrypted values into mySql database.
* Overall, this project provides a practical demonstration of symmetric encryption using MCRYPT in Kali Linux, empowering users to enhance the security of their files through robust encryption techniques

**Table Of Content**

|  |  |  |
| --- | --- | --- |
| **CHAPTERS** | **DESCRIPTION** | **PAGE NUMBERS** |
| 1 | INTRODUCTION | 2 |
| 1.1 | AIM | 3 |
| 1.2 | SCOPE | 4 |
| 2 | LITERATURE REVIEW | 6 |
| 3 | EXISTING SOLUTIONS | 8 |
| 4 | PROPOSED SYSTEM | 11 |
| 4.1 | REQUIREMENT ANALYSIS | 12 |
| 4.1.1 | HARDWARE REQUIREMENTS | 12 |
| 4.1.2 | SOFTWARE REQUIREMENTS | 12 |
| 4.2 | MERITS AND DEMERITS | 13 |
| 5 | DESIGN DESCRIPTION | 15 |
| 5.1 | CONCEPTUAL DESIGN | 15 |
| 6 | IMPLEMENTATION AND DISCUSSION | 16 |
| 6.1 | IMPLEMENTATION | 17 |
| 7 | RESULT | 20 |
| 8 | CONCLUSION AND FUTURE ENHANCEMENT | 21 |
| 8.1 | CONCLUSION | 21 |
| 8.2 | ENHANCEMENT | 21 |
| 8.3 | REFERENCES | 24 |

# CHAPTER 1

1

#### INTRODUCTION

This program provides a simple interface for encrypting and decrypting user passwords using the AES- 128 encryption algorithm in CBC mode, utilizing the Mcrypt library. It offers the following functionalities:

* **User Input:** Users can securely input their email and password.
* **Encryption:** The entered password is encrypted with a fixed key and initialization vector (IV), padded appropriately, and the encrypted data is displayed in hexadecimal format.
* **Decryption:** The program can decrypt a previously encrypted hexadecimal password back to its original form.
* **Interactive Menu:** Users interact with the program through a menu-driven interface, allowing them to choose between entering credentials, encrypting the password, decrypting the password, or exiting the program.

This approach ensures that sensitive information such as passwords can be securely managed and protected

#### AIM

* The aim of this program is to provide a secure and user-friendly application for managing sensitive user information, specifically focusing on the encryption and decryption of user passwords.
* The program ensures secure data storage by encrypting user passwords with AES-128 in CBC mode using the Mcrypt library, thus protecting them from unauthorized access. It also allows for the decryption of these passwords, ensuring that only authorized users can retrieve the original passwords when necessary.
* The application features an intuitive menu-driven interface, enabling users to input their credentials, encrypt their passwords, and decrypt them as required.
* Additionally, the program serves an educational purpose by demonstrating the practical implementation of AES-128 encryption, emphasizing secure password handling practices in software development.

#### SCOPE

* **User Authentication:** Facilitates secure handling of user credentials by encrypting passwords before storage, ensuring they are not stored in plain text.
* **Data Security:** Implements AES-128 encryption in CBC mode to protect sensitive information, making it suitable for applications requiring high security standards.
* **Interactive User Interface:** Provides a menu-driven interface that allows users to easily input their credentials, encrypt passwords, and decrypt them as needed, enhancing user experience and accessibility.
* **Educational Demonstration:** Serves as an educational tool to demonstrate the implementation of encryption and decryption processes using the Mcrypt library in C, offering practical insights into secure programming practices.
* **Potential Integration:** Can be integrated into larger systems or applications that require secure password management, acting as a foundational component for secure data handling.
* **Customizability:** Allows for modifications and extensions, such as incorporating different encryption algorithms, dynamic key and IV generation, or integration with more complex authentication systems.
* **Security Practices:** Highlights the importance of secure password storage and management, promoting best practices in software development for enhanced data security.

# CHAPTER 2

#### LITERATURE REVIEW

1. **AES: The Advanced Encryption Standard by Joan Daemen and Vincent**

**Rijmen - 2001**

This foundational paper introduces the AES (Rijndael) algorithm, detailing its design principles, security features, and performance characteristics. It is a cornerstone of modern cryptography and widely referenced in the field.

1. **New Directions in Cryptography by Whitfield Diffie and Martin E. Hellman - 1976**

A classic paper that introduced the concept of public key cryptography and laid the foundation for modern cryptographic practices. While focused on public key cryptography, it also provides context for the evolution of secure communication techniques.This landmark paper introduced the concepts of public key cryptography and digital signatures, which have had a profound impact on the field of cryptography.

# 

# CHAPTER 3

#### EXISTING SOLUTION:

1. **OpenSSL :**

OpenSSL is a powerful, full-featured open-source toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It includes a cryptographic library that supports various encryption algorithms, including AES.

****

**Fig 3.1: OpenSSL**

1. **Libsodium:**

Libsodium is a modern, easy-to-use software library for encryption, decryption, signatures, password hashing, and more.



**Fig3. 2:** Libsodium

##### bcrypt:

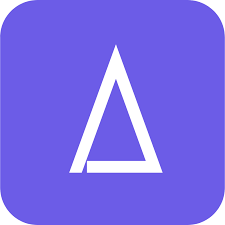
bcrypt is a password hashing function designed for securely storing passwords. It incorporates a salt to protect against rainbow table attacks and allows for a configurable number of iterations to adjust computational cost.



**Fig 3.3: bcrypt**

1. **Argon2 :**

Argon2 is the winner of the Password Hashing Competition (PHC) and is designed to be memory-hard, making it resistant to GPU-based attacks.



**Fig 3.4 : Argon2**

# CHAPTER 4

#### PROPOSED SYSTEM

The proposed system is that enables the user to encrypt and decrypt data. First the user is prompted

to enter the username and password, the user is then given an option to be shown the encrypted or decrypted text based on his or her choice.

For encryption and decryption of text we had used AES in CBC mode with Mcrypt Library and for the programming language we used C language.

If we had to use any other programming language we could use Java, as it requires Maven project to be implemented and the use of BouncyCastle dependencies to encrypt and decrypt data, and storing the encrypted values into encrypted\_values table in mySql db.

#### REQUIREMENT ANALYSIS

##### Software Requirements

* + - * Windows 7 or later, Linux, or macOS
      * Mcrypt Library - AES Encryption
      * C Compiler

##### Hardware Requirements

* + - * System 32 or 64 bit with 4 GB or 8 GB RAM
      * CPU
      * RAM



**Fig 4.1 : Kali Interface**

##### MERITS AND DEMERITS Merits:

* + - * Simplicity
      * User-Friendly Interface
      * Customization
      * Padding Handling

##### Demerits:

* + - * Security Concerns (if Not Properly Secured)
      * Limited Flexibility
      * Not - Production ready

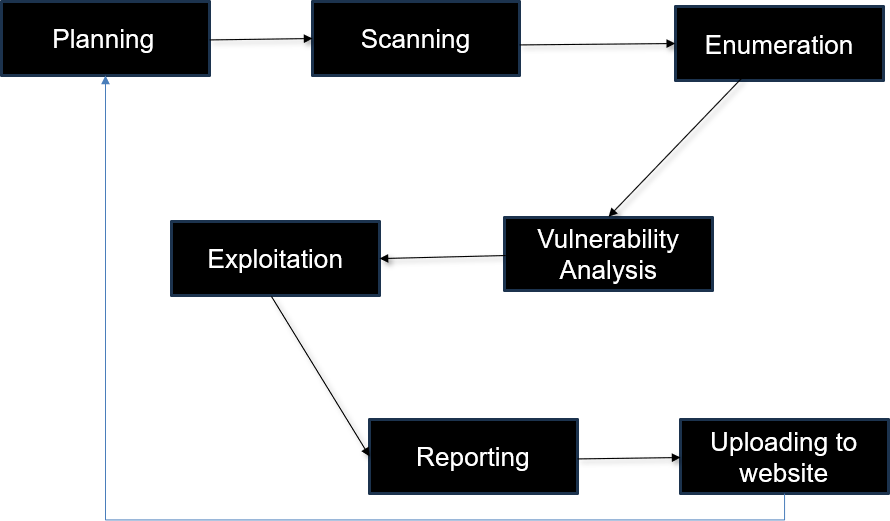
# CHAPTER 5

14

#### DESIGN DESCRIPTION

##### 5.1 CONCEPTUAL DESIGN

The diagram shows the steps involved in



**Fig 6:** Steps for VAPT

# CHAPTER 6

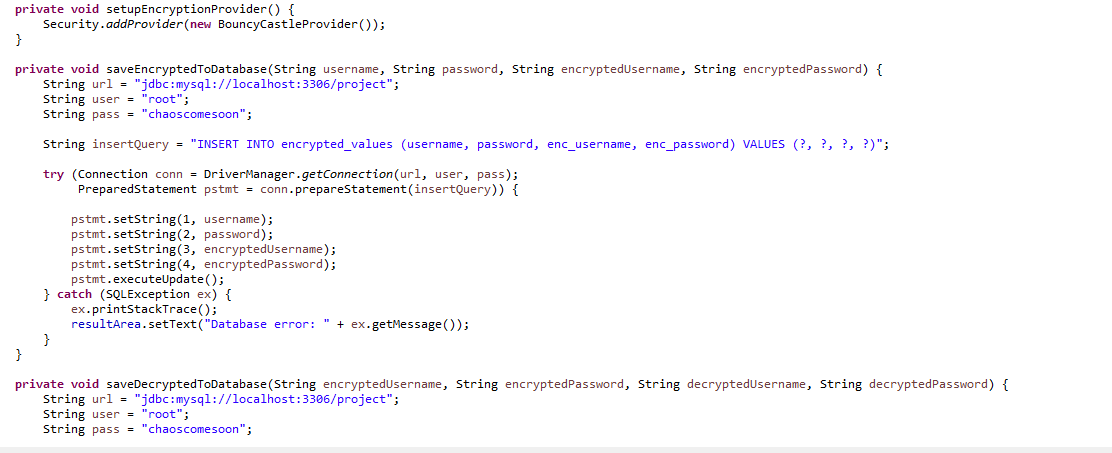
#### IMPLEMENTATION AND DISCUSSION

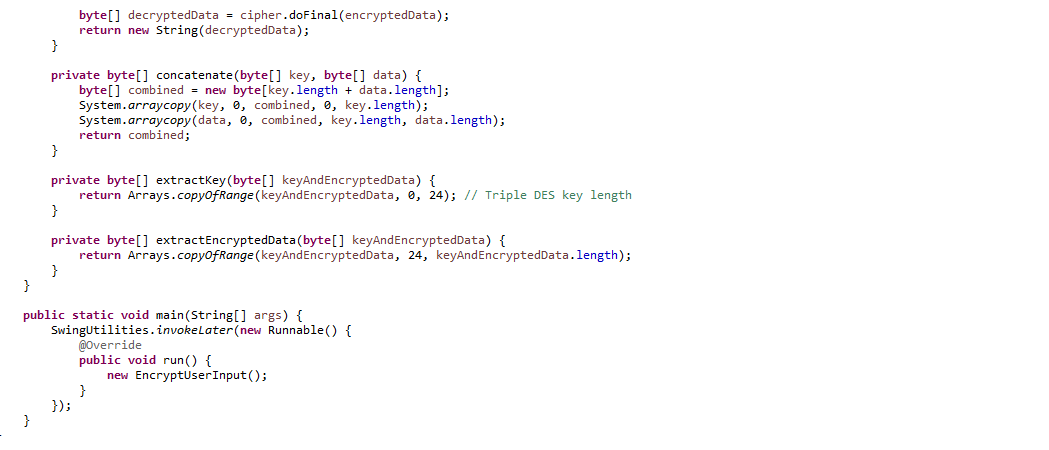
**3.1 IMPLEMENTATION**

### Open Eclipse-IDE :

### **Fig 7:**Scanning

**Fig 7:**Scanning

**Fig 7:**Scanning

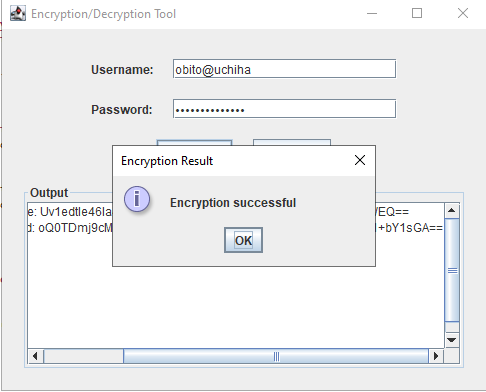


**Fig 7:**Scanning

**CHAPTER 7**

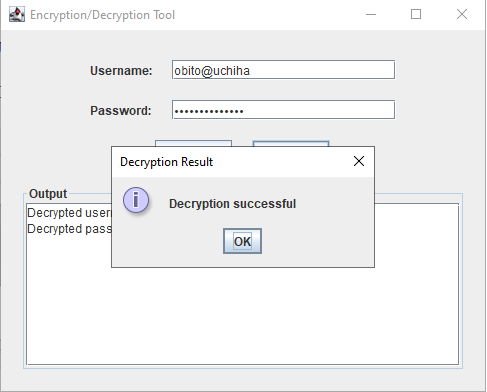
**OUTPUT:**

ENCRYPTION:

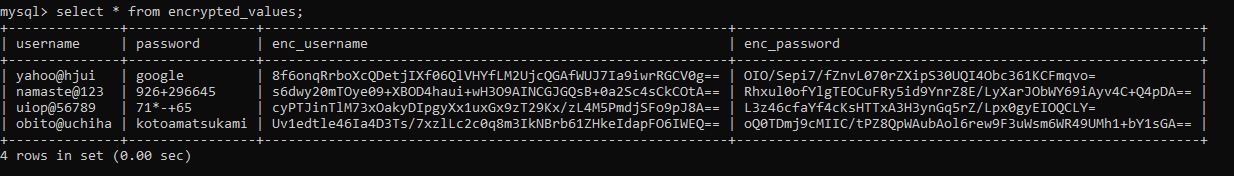


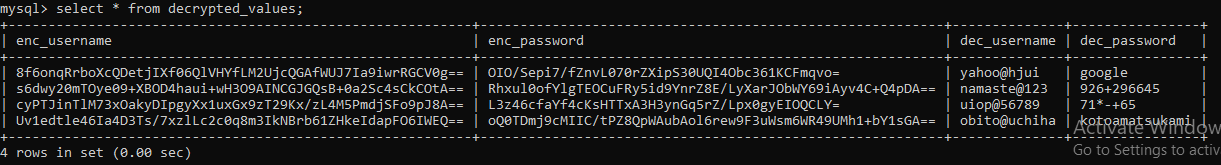
**Fig 7.1**:encryption

DECRYPTION:



**Fig 7.2** : decryption





**Fig 7.3: MySql Table**

# 

# CHAPTER 8

#### CONCLUSION AND FUTURE ENHANCEMEMT

##### 8.1. CONCLUSION

* In conclusion,by using the AES in CBC mode with Mcryt library maintains a sense of confidentiality of the user and the data it holds.
* Prioritizing security has equipped us to protect our data and operations
* This project serves as a foundation for continuous improvement and commitment to security.
* Thanks to the team members and faculty for their dedicated efforts.

##### FUTURE ENHANCEMENTS

* It requires quite a few enhancements to be secure, robust, and suitable for production use. By addressing the identified issues and following best practices in cryptographic implementations, the code can be transformed into a more secure and reliable solution.

#### REFERENCES

1. Daftry, A., M. (2019). "A Comprehensive Study on Vulnerability Assessment and Penetration Testing." International Journal of Computer Applications, 975, 8887.
2. Alhazmi, A., & Malaiya, Y. (2018). "A Survey on Vulnerability Assessment and Penetration Testing of Cloud Computing Environment." International Journal of Network Security & Its Applications (IJNSA), 10(2), 69-84.
3. Baloch, S., & Ahmed, J. (2020). "An Approach for Automated Vulnerability Assessment and Penetration Testing." International Journal of Advanced Computer Science and Applications, 11(6), 158-163.
4. Subramanian, S., & Kumar, R. (2017). "A Survey on Penetration Testing and its Techniques." International Journal of Advanced Research in Computer Science, 8(5), 283-287