**PROJECT DOCUMENTATION SUBMITTED TO TECHIONARY**



PASSWORD MANAGER USING CRYPTOGRAPHIC TECHNIQUES

PROJECT DATE: 01-07-2020

BATCH NO: MLI - 22

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TEAM MEMBERS** | | | | |
| **S No** | **NAME** | **ROLE** | **COLLEGE** | **CONTACT NO** |
| 1 | Mohammed Abdus Samee | Team Lead | Gokaraju Rangaraju Institute of Technology | 9963868701 |
| 2 | P Bharat Kumar | Team Member | Vignan’s Institute of Information Technology | 6305123856 |
| 3 | G Aravind | Team Member | Mallareddy College of Engineering and Technology | 9290126038 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PREPARED BY** | Abdus Samee, Aravind, Bharat | **TITLE** | Password Management using Cryptographic Techniques. | **DATE** | 01-07-2020 |
| **GUIDED BY** | Rajesh sir | **TITLE** | Password Management using Cryptographic Techniques. | **DATE** | 21-07-2020 |

Acknowledgement

I thank Techionary, for providing me an opportunity to do the project work on Password Management using Cryptographic Techniques and giving us all support and guidance, which made me complete the project duly.

I am extremely thankful to Adnaan Arbaaz Ahmed, CTO and Director, Techionary for providing such a nice support, guidance and monitoring project progress accordingly by taking out the tike from his busy schedule of managing the corporate affairs.

I owe my deep gratitude to our project guide Rajesh, who took keen interest on our project work and guided us all along, till the completion of our project work by providing all the necessary information for developing a good system.

I would not forget to remember Rajesh, Raj Kumar, of Techionary for their encouragement and more over for their timely support and guidance till the completion of our project work.

I am thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staffs of Computer Science which helped us in successfully completing our project work. Also, I would like to extend our sincere esteems to all staff in laboratory for their timely support.

Table of Contents

[PROBLEM STATEMENT](#_1fob9te) 4

[PROJECT SCOPE](#_3znysh7) 4

[PRODUCT OR SYSTEM FEATURES AND REQUIREMENTS](#_2et92p0) **5**

[PROJECT SUCCESS CRITERIA](#_tyjcwt) **5**

1. [STATEMENT OF WORK](#_3dy6vkm) **6**

1.1 [SCOPE OF WORK](#_1t3h5sf) **6**

1.2 [LOCATION OF WORK](#_4d34og8) **6**

1.3 [PERIOD OF PERFORMANCE](#_2s8eyo1) **6**

1.4 [SCHEDULE](#_17dp8vu) **7**

1.5 [STANDARDS FOLLOWED](#_3rdcrjn) **8**

1.6 [ACCEPTANCE CRITERIA FOR USERS](#_26in1rg) **8**

1.7 [ADDITIONAL REQUIREMENTS](#_lnxbz9) **8**

# PROBLEM STATEMENT

Problems faced by the users while using the current system

|  |
| --- |
| Password manager stores password using encryption techniques to secure the password. Passwords are key aspects for everything to protect our user accounts from potential hackers. Most of the password management techniques used now a days are made by symmetric cryptographic technique, as it has a major flaw of using public keys at the user end as well as the receiver end. The hash function has also failed in terms of protecting the user data. By using the Asymmetric Cryptographic Techniques, there are  few algorithms which generate separate keys for user and receiver end.  For most of the asymmetric techniques, has limited the size of the bit key to a lesser size. So, it is not as safe as encrypting the text using a higher bit key. |

# PROJECT SCOPE

Project Purpose and Justification

|  |
| --- |
| The main scope of the project is storing the cipher text using a large bit key so that it takes a lot of time when hacker try to retrieve the password. So, we have developed the password manager that will generate new key and new ciphertexts are created after a user has accessed it for multiple times. By this, every password which is stored , will be more secure form getting deciphered. |

# PRODUCT OR SYSTEM FEATURES AND REQUIREMENTS

|  |
| --- |
| 1. Python 3 2. Oracle Database 3. Python libraries: Pycryptodome and cx\_Oracle |

# PROJECT SUCCESS CRITERIA

|  |
| --- |
| As the algorithm written and developed by as generate a specific private key for the users and also protect their credentials, we think as we have used a Large bit key to generate and store the data it keeps the users safe from the potential threats. |

# STATEMENT OF WORK

## SCOPE OF WORK

|  |
| --- |
| The major scope of this project is to protect the user credentials by generating a new private key after the user has accessed it multiple times. As other cryptographic techniques does not use a separate public and private key they are less preferable as anyone can decrypt the data easily. So our private key keeps changing and is more secure than the other cryptographic techniques that are currently available. |

## LOCATION OF WORK

|  |
| --- |
| The work on the code as well as implementation of the other things are done virtually. |

## PERIOD OF PERFORMANCE

|  |
| --- |
| The Algorithm written by us works successfully by taking the message and encrypting the data and storing the data in a safe manner. |

## SCHEDULE

|  |  |  |  |
| --- | --- | --- | --- |
| **CATEGORY/TASK** | **WORK DONE** | **START DATE** | **END DATE** |
| Phase 1 – Planning |  |  |  |
| Task A | Understanding the problem statement and gathering requirements | 1-07-2020 | 2-07-2020 |
| Task B | Understanding RSA cryptographic algorithm | 3-07-2020 | 06-07-2020 |
| Phase 2 – Execution |  |  |  |
| Task A | Installing python ,oracle database, and installing python libraries such as pycryptodome, cx\_Oracle. | 6-07-2020 | 07-07-2020 |
| Task B | Connecting database by using python | 8-07-2020 | 9-07-2020 |
| Phase 3 – Monitoring |  |  |  |
| Task A | Implementation of RSA algorithm | 10-07-2020 | 12-07-2020 |
| Task B | Executing the RSA algorithm | 13-07-2020 | 15-07-2020 |
| Phase 4 – Closing |  |  |  |
| Task A | Verifying the correctness of the algorithms by giving input | 16-07-2020 | 18-07-2020 |
| Task B | Connecting entire project to the database and correcting the errors | 19-07-2020 | 20-07-2020 |

## STANDARDS FOLLOWED

|  |
| --- |
| Oracle 11g database |

## ACCEPTANCE CRITERIA FOR USERS

|  |
| --- |
| This Password Manager generates new key and creates new ciphertexts for all the passwords that are stored after the database is accessed multiple times. This prevents the attackers from deciphering the ciphertext. |

## ADDITIONAL REQUIREMENTS

|  |
| --- |
|  |

CONCLUSION

Our project is Password Manager which stores passwords using cryptographic techniques.

It uses RSA algorithm to encrypt the data and stores the ciphertext in the database. The key changes after the database is accessed multiple times.

The programing language we have used is Python. We chose python as it is an easy programming language with broad stand library for us to use from and it is also portable and interactive.

Our project is very efficient in managing passwords securely.

REFERENCES

RSA Encryption Implementation: <https://pycryptodome.readthedocs.io/en/latest/>

Oracle Database Connections: <https://cx-oracle.readthedocs.io/en/latest/index.html>