**School of Computing Sciences**

**Department of Computer Science and Engineering**

**Academic Year: 2020-2021**

**REPORT SUBMITTED FOR FIRST REVIEW**

**BATCH No: 56**

**Project Title: CAESER CIPHER FOR EFFICIENT DATA PRIVACY AND SECURITY**

|  |  |
| --- | --- |
| **STUDENT NAME(S)** | **REGISTER NUMBER(S)** |
| **V.LAHARI** | 17113143 |
| **DINESH UDAYAN** | 17113255 |
| **TANUJA SUTRADHAR** | 17113258 |
|  |  |

**Supervisor Name: DR. P.N. RENJITH**

TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| Sl. No | Content | Page No |
| 1 | Project Description (Minimum 200 words) | 3 |
| 2 | Literature Survey – Tabular Form | 3 |
| 3 | Software Requirements | 4 |
| 4 | Hardware requirements | 4-5 |
| 5 | Project Plan & Individual role | 5-6 |
| 6 | Partially completed Technical paper   1. Introduction – Minimum 300 words 2. Literature review – Minimum 500 words | 6-7 |
| 7 | Guide Approval  (Signature in hard copy or print of Mail approval for   1. PPT 2. Partially completed technical paper   ) | 7 |

**1.Project Description**

We aim to design a multi-layered encryption algorithm which will be carried out in particular a sequence. The timestamp of the fetch request will be taken as the key of the inner most layer. The timestamp captured will be manipulated to generate the first key of the inner most layer.

The geo-location of the sender is also noted at every request made by the user and will be considered as the middle layer. Using cryptographic network communication, we receive the IP address of the sender. This IP address will help to generate the final key for the outer most layer and also used for verification purpose. These 3 factors together will provide a unique key for the entire encryption.

After the encryption, we plan to send the data along with key by following the TCP/IP protocol approach to carry forward the decryption process.

**2.Literature Review:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Title of the Papers: | Authors: | Name of the conference/journal and year of publication: | Methodology: | Issues/  Limitations: |
| An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher  Publisher: IEEE | Deepanshu Gautam  Parth Sharma  Poonam Saini  Chandan Agrawal  Dr Munish Mehta | 2nd International Conference on Trends in Electronics and Informatics (ICOEI)  2018 | Performing encryption by using the poly alphabetic cipher techniques and the vigenere table. | If the length of the text is small, keys will be repeated treating it as interwoven caeser text which can be easily broken . |
| Multi-Layered Encryption Method | Usman Sudibyo  Cinantya Paramita | 3rd International Conference on Informatics and Computational Sciences (ICICoS)  2019 | Implementing basic encryption algorithm to create a complex one for performing multi-layered encryption. | The key generation method remains constant making it vulnerable. |
| Analysis of Encryption Algorithms (RSA, SRNN and 2 Key Pair) for Information Security | Sarika Y. Bonde  Prof.Dr. U. S. Bhadade | [International Conference on Computing, Communication, Control and Automation (ICCUBEA)](https://ieeexplore.ieee.org/xpl/conhome/8443317/proceeding)  [2017](https://ieeexplore.ieee.org/xpl/conhome/8443317/proceeding) | Performing encryption using RSA, SRNN  And 2 key pair algorithm. | RSA algorithm is very slow and takes longest time for encryption. |
| Caesar Cipher with Goldbach Code Compression for Efficient Cryptography | Jan Carlo T. Arroyo , Allemar Jhone P. Delima | International Journal of Emerging Trends in Engineering Research  2020 | Use Goldbach code algorithm to conceal the ciphertext generated by the Caesar cipher | It will require resources like memory, speed and thus concern the space complexity. |

**3.SOFTWARE REQUIREMENTS**

* Operating System : Windows 7 or higher
* Programming : Python 3.8 and related libraries
* Software : vs code

**4.Hardware Requirements**

* Processor : Any Processor above 500 MHz.
* Ram : 1 GB
* Hard Disk : 1 GB
* Input device : Standard Keyboard and Mouse.
* Output device : VGA and High Resolution Monitor.

**5.Project Plan**

**Phase 1:-** Collection of required libraries as per the algorithm and getting the input field to carry out the declaration.

**Phase2:-** Encryption and decryption output.

**Phase3:-** Transfer of the key.

**Phase4:**- Testing all test cases.

**Individual Role**

V. Lahari- Transferring algorithm.

Dinesh Udayan – Hard coding (Final Desktop Application)

Tanuja Sutradhar– Encryption Decryption process