IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Design & Implementation of Unpacker From file Packer Using Cryptographic Algorithm

Mahesh Mokashe Rushikesh Godase Shubham Hambarde Shivani Deshmukh

Abstract File packing and unpacking is a fundamental concept in many aspect of computer science, as it is involved in many applications Even if you don't actually feel, a lot of operations inside the computer is happened. This project is used to perform packing and unpacking activity for multiple types of files for security purpose we using cryptographic algorithm for encryption and decryption of data present in file.

In a File system, data security plays a major role Encryption is the method of transforming the original texted message into an unknown form. Decryption is the method to transform the encrypted data into the original form. The purpose of this study was to pack the multiple files into single packed file by encrypting original data and when we unpack the file create new files by decrypting the data. This project is used to perform packing and unpacking activity for multiple types of files.

In case of Packing activity me maintain one file which contains metadata and data of multiple files from specified directory. In case of Unpacking activity we extract all data from packed files and according to its metadata we create all files. In this project we have to use Java as Front end as well as Backend for platform independency. So this project used object oriented programming with the Java2 Standard Edition (J2SE) programming language.

Keywords: Cryptography; Encryption; Decryption; DNA Algorithm

1.INTRODUCTION

Cryptography is the art of secret writing. Cryptography is the creativity of translating the original plain text in to cipher text. The sender translate the plaintext in to cipher text .This cipher text is then sends to the receiver. The authorized receiver gets the cipher text and then convert the cipher text back in to the original form. The main aim of the cryptography is to protect the information from illegal access. The data can be read in its original form is called plain text. The way of mask the plain text in such a way as to hide its original form is called encryption. The method of encrypting the plain text which results in unreadable form is called cipher text. The method of taking encrypted message or data and converting back into the text in to its original form is called decryption. An entity which provides encryption and decryption is called cryptosystems. . Cryptography plays a vital role in security aspect. It provides many security goals to make sure the secrecy of data. Cryptography is the art of sending the information in a protective way .And ensuring that the legitimate person can able to access the information. Because of the efficient usage of networking we can transmit the information from one location to another location over the internet.

1.1 PROJECT IDEA

Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Description: Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.1.2 MOTIVATION OF THE PROJECT

- Thus our main motivation is to find the solution over an it. Where, our system will provide security to packed files data by using cryptographic algorithm.
- The proposed cryptographic algorithm should be efficient and the system will be scalable. Through this research it is highlighted that securing data of files .
- Drawbacks of the existing system motivated us to design a better user-friendly tool.

2. LITERATURE SURVEY

1. SACA: A STUDY OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS 2020 : Muhammad Aamir Panhwar , Sijjad Ali khuhro , Ghazala Panhwar , Kamran Ali memon In this paper, the idea of cryptography is described. Cryptographic area essentially has Two types of parts: symmetrical and asymmetric. The symmetric algorithm uses the same key

for encryption and decryption, while the asymmetric algorithm uses a different key for encryption and decryption

2. DESIGN AND IMPLEMENTATION OF A FILE SPLITTER AND MERGER SOFTWARE 2019 : Muhanad Hayder The system runs on all existing operating systems, because Java is platform independent. System implementation, make the task easier for users to deal with such kind of functionality wasn‟t proposed in user friendly GUI before. The system is almost error free as we handled all exceptions that will catch every possible error .
3. A STUDY ON SYMMETRIC AND ASYMMETRIC KEY ENCRYPTION ALGORITHMS S.Suguna1, Dr.V.Dhanakoti,R. Manjupriya 2020

3. PROBLEM DEFINATION AND SCOPE

3.1 PROBLEM STATEMENT

In a File system, data security plays a major role Encryption is the method of transforming the original texted message into an unknown form. Decryption is the method to transform the encrypted data into the original form
The purpose of this study was to pack the multiple files into single packed file by encrypting original data and when we unpack the file create new files by decrypting the data.

3.1.1 GOALS AND OBJECTIVES

1. The main objective of this system to use cryptography for data security of files.
2. User can select particular extension files to pack also(like .c only)
3. Another main objective of this project is to maintain user's source code file(c/cpp/java etc) by packing it into single file and then according to user's will he will able to unpack this packed file.
4. Security is provided to user's data using cryptographic algorithms

3.2 STATEMENT OF SCOPE

The software requirement specification document enlists enough and necessary requirements that are re-quired for the project development. To derive the requirements, we need to have clear and thorough understanding of products to be developed or being develop. This is achieved refined with detailed and continuous commune- cation with the project team and customer till the completion of the software. The SRS may be one of a contract deliverable Data item Description or have other forms of organizationally mandated content.

3.3 METHODOLOGIES OF PROBLEM SOLVING AND EFFICIENCY ISSUES

A. Brief Introduction on RSA and Public-key Cryptograph
Rivest-Shamir-Adleman (RSA) RSA is widely used Public-Key algorithm. RSA firstly described in 1977. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. The key feature of public-key cryptosystem is that the encryption and decryption procedure are done with two different keys - public key and private key, and the private key can not be derived from the public key, that enables the publication of the encryption key without the risk of leaking the secrets The most significant approach of public key cryptography algorithm is RSA, which can resist almost all the known passwords attacks so far. RSA algorithm, which is named after the inventors, is the first algorithm that can be used both for data encryption and digital signatures RSA algorithm's security depends on the difficulty of decomposition of large numbers. In the algorithm, two large prime numbers are used for constructing the publickey and the private-key. It is estimated that the difficulty of guessing the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime numbers. RSA algorithm has been used as a possible authentication methods in ISAKMP / Oakley framework. Diffie-Hellman key exchange algorithm is a key component of the framework. In the beginning of a key agreement session, participants communicate by using Diffie-Hellman algorithm and create shared keys which will be used for key agreement protocol of follow-up steps.

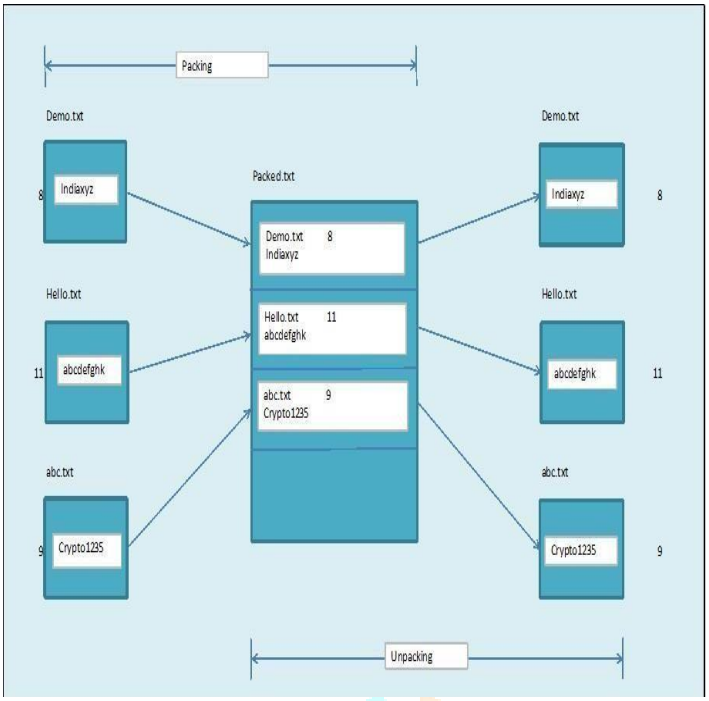
3.4 OUTCOME

- Cryptography is the science of using mathematics to encrypt and decrypt data.
- The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient

3.5 APPLICATION

- Secure communications
- End-to-end Encryption
- Storing Data
- Storing Passwords
- Cryptography is hard

4. DETAILED DESIGN



5. SUMMERY AND CONCLUSION

5.1 SUMMERY

- The strength of the keys and the effectiveness of mechanisms and protocols associated with the keys; and
- he protection of the keys through key management (secure key generation, storage, distribution, use and destruction).
- Strong algorithms combined with poor key management are as likely to fail as poor algorithms embedded in a strong key management context.
- Cryptography is a type of a rule or a technique by which private or sensitive information is secured from the public or other members. It focuses on the confidential data, authentication, data integrity etc. The use of Cryptography in passwords is a very famous example.

5.2 CONCLUSION

- Packing and unpacking these are main functionality provided. Here , for security purpose we are using cryptographic algorithm for data encryption and decryption.
- Cryptography plays a vital role in security aspect. It provides many security goals to make sure the secrecy of data. Cryptography provides many advantages so it is widely used nowadays.
- Encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality.

6.REFERENCES

[1] " The complete reference JAVA " by Herbert Schieldt

[2] Bruce Eckel, President, Mind View, Inc., Thinking in Java,2nd Edition, Prentice Hall, Release 11 mid-June, 2000

[3] Pushpa, B. R. (2017). A new technique for data encryption using DNA sequence. 2017 International Conference on Intelligent Computing and Control (I2C2).

[4] Akiwate, B., & Parthiban, L. (2018). A Dynamic DNA for Keybased Cryptography. 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS).

[5] Sable Nilesh Popat*, Y. P. Singh," Efficient Research on the Relationship Standard Mining Calculations in Data Mining" in Journal of Advances in Science and Technology | Science & Technology, Vol. 14, Issue No. 2, September-2017, ISSN 2230-9659.

[6] Sable Nilesh Popat*, Y. P. Singh," Analysis and Study on the Classifier Based Data Mining Methods" in Journal of Advances in Science and Technology | Science & Technology, Vol. 14, Issue No. 2, September-2017, ISSN 2230-9659.