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

Rushikesh Godase Mahesh Mokashe 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.

I. 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.

A. RELATED WORK

4.4.3 CLASSIFICATION OF CRYPTOGRAPHY

Depending upon the key cryptography can be divided into two categories.

- Symmetric encryption(Private key)
- Asymmetric encryption(Public key)

A. Symmetric Encryption (private key Encryption) During the encryption and decryption process the same key is used at the sender and receiver site. Before the Transmission of information starts the key distribution has to be made [2]. Example: DES, 3DES, BLOWFISH, AES etc.

B. Asymmetric Encryption (Public key encryption) In Asymmetric encryption, two different keys are used for encryption and decryption process. At the same time the two keys are generated. In that one key is transferred to other side before the exchange of information begins [3]. Example: RSA, Elgamal, Elgamal signature Diffie Hellman key exchange, Digital signature

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

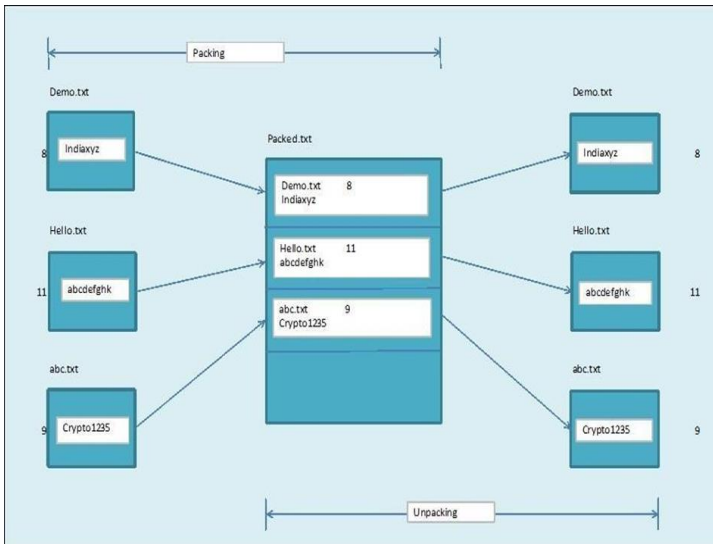
II. PROPOSED SYSTEM

A software requirements specification (SRS) is a description of a software system to be developed, laying out function and non-function requirements, and may include a set of use cases that describe interaction the users will have with the software. Software requirement specification establishes the basis for an agreement between customer and contractor or suppliers (in market-driven projects, these roles may be played by the marketing and development division) on do. Software requirement specification permits a rigorous assessment of requirements before design can begin and reduces later redesign. It should also provide a realistic basis for estimating product costs, risks, and schedules.

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. .

It 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.

System Design



III. ALGORITHMS

(A) THE RSA CRYPTOSYSTEM

RSA cryptosystem uses the mode n, the smallest nonnegative complete the remaining lines of operation, where n is the product of two different primes p and q . RSA algorithm is described as following

1) Randomly generates two primes P and Q of length K / 2 bit ;

2) Calculate the public key publicKey=P*Q; (public Key's length is k-bit)

3) Generate a random encryption key keyE, 2<=keyE<=

<D(n)-I, where GCD(keyE, <D(n))=I;

This is the necessary and sufficient conditions for solvability of the decryption key keyE * keyD mod <D(n)=I, <D(n) is known as the Euler function of n, the value is <D(n)=(P-1)*(Q-l)

4) Calculate the decryption key, keyD=keyE-l mod (n) ,keyE-l is inverse for the decryption key keyD. The formula of the original equation is keyE * keyD mod <D(n)=1

Now, the public key, encryption key and decryption key are all created.

Then, the process of encryption of the plaintext and decryption of ciphertext is as follows:

1.Encryption: C = MkeyE mod publicKey; where M is plaintext, C is ciphertext.

2.Decryption: M = CkeyD mod publicKey; in which M plaintext, C is ciphertext.).

(B) The Implementation Of RSA:

To implement RSA cryptosystem is a rather complex process, which involves the generation of prime numbers, large integer modular arithmetic and other mathematical calculations. In RSA cryptosystem, p and q are large prime numbers. To achieve it, the most important factor is the efficiency in generate large prime numbers.

Normally, probabilistic algorithms are adopted in generate large prime numbers. This should be: p, q are large prime numbers, when seeking primes p and q with the method of factorization, then the difficulty is actually the same as to attack to RSA (the decomposition of large composite number) , it's feasible as to the computer .

In general, probabilistic algorithms do not focus on generating prime numbers, but first randomly generate a large odd number, then determine whether this odd integer is a prime number with probabilistic algorithms (this process is commonly referred to as Primarily Test .

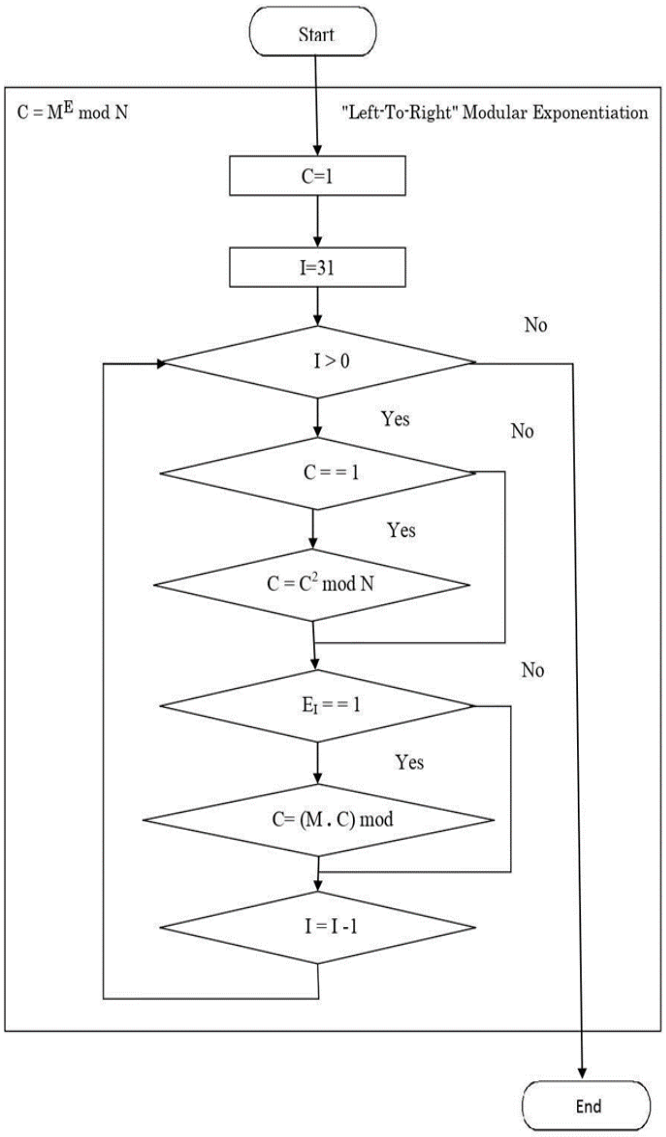


Fig :- RSA Encrpytion & Decryption

Swings

Swings is a set of packages built on top of the awt that provides you with a great number of prebuilt classes.

There many UI components are:- JButton

- JCheckBox
- JFrame
- JDialog
- JEditorPane
- JFileChooser
- JLabel And many more

IV:- CONCLUSION AND FUTURE WORK

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, We gave user-friendly Graphical user interface using java AWT/Swing.

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.

The encryption and decryption solution can ensure the confidentiality of the information, as well as the integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting. 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.

This project contains a complete discussion of the cryptography, encryption, decryption, and RSA public key and other related technology applications in the

military, business, privacy and other fields of information security which plays an important role. Problem for RSA encryption on the file, it indicates the RSA mathematical algorithms in the computer industry's importance and its shortcomings. It discusses the questions of how to apply to the personal life of RSA information security issues. And also contains the use of RSA and the basic principles of data encryption and decryption. In the end, it proposed a new program to improve RSA algorithm based on RSA cryptography and the extensive application .In summary, this issue of the RSA encryption and decryption keys, RSA algorithm, the new use of the RSA and other issues to study and make some new programs, future work should be in the new RSA cryptographic algorithms and a wide range of applications continue to research.

V. REFERENCES

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

[2]Bruce Eckel, President, MindView, Inc., Thinking in Java,2nd Edition, PrenticeHall,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).