IPHV1I20014X

International Journal Of Advanced Research and Innovations Vol.1, Issue .2

ISSN Online: *2319 – 9253*

Print: *2319 – 9245*

Encryption/Decryption Application

Niteesh Kumar[1], K.Sameer Kumar[2], B.Sanjay kumar[3], T.Venkata Ramana[4]

[1,2]Computer Science Department, SLC's Institute of engineering and Technology

[3]Computer Science Department, spoorthy engineering college

[4] Professor & Head, Department of CSE, SLC'S IET.

Abstract

This paper presents about Encryption/Decryption application that is able to work with any type of file; for example: image files, data files, documentation files…etc. The method of encryption is simple enough yet powerful enough to fit the needs of students and staff in a small institution. Our application uses simple key generation method using AES (Advance Encryption Standard) algorithm. The key generation and Encryption are all done by the system itself after clicking the encryption button with transparency to the user. The same encryption key is also used to decrypt the encrypted binary file i.e. Symmetric key encryption is used.

Keywords— **Encryption , Decryption,AES,Security,Files**

Introduction

Encryption is the most effective way to achieve data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data. Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data. The unencrypted data is referred to as the plaintext and the encrypted data as the cipher text, which is representation of the original data in a different form.

Key-based algorithms use an Encryption key to encrypt the message. There are two general categories for key-based Encryption: Symmetric Encryption which uses a single key to encrypt and decrypt the message and Asymmetric Encryption which uses two different keys – a public key to encrypt the message, and a private key to decrypt it. Currently, there are several types of key based Encryption algorithms such as: DES, RSA,

International Journal Of Advanced Research and Innovations Vol.1, Issue .2
ISSN Online: *2319 – 9253*
Print: *2319 – 9245*

PGP, Elliptic curve, and others but all of these algorithms depend on high mathematical manipulations.

I. METHODOLOGY

AES is an iterated block cipher with a fixed block length of 128 bits and a variable key length that can be 128, 192 or 256 bits. The algorithm, shown in Figure, passes plain text through a number of round transformations to produce the cipher. The algorithm allows 10, 12, or 14 transformations, depending on the key length. Each round transformation is composed of three distinct transformations, called layers. The first is the non-linear layer, Sub Bytes, which interchanges blocks of bytes within the word. The second is the linear mixing layer (Shift Rows + Mix Columns), and the third is the key addition layer (Add Round key). The transformations are invertible, allowing the cipher text to be converted back to plain text if one has the key.

The approximate time of encryption , decryption and size of encrypted file is in table I.

Table I

Original Size(kb)	Encrypted size(kb)	Encryption time(ms)	Decryption time(ms)
2	5	862	1025
25	62	1,231	1,321
70	112	3,841	7,231

II. FILE TYPES

There are no limitations of the type of files accepted for encryption in this application, which means any type of a file such as data files, audio files, video files or image files can be encrypted by the application. This is because all the files are encrypted at the binary level. There is also no limitation of the size of the file that can be encrypted using this application, which provides flexibility to the user. The encrypted file can only be opened and viewed after it has been decrypted to its original file using the symmetric encryption key.

III. FEATURES

- The interface of the application is simple enough to be used by any user
- The encryption is performed simply by choosing any file while decryption is executed by choosing an encrypted file with an appropriate key.
- The encrypted file is given with a unique extension .SNS which can be easily distinguishable from other files

International Journal Of Advanced Research and Innovations Vol.1, Issue .2
ISSN Online: *2319 – 9253*
Print: *2319 – 9245*

and only the files with that extension will be decrypted.

- Encryption/Decryption will work with any file type (documents, image, videos, ppt's ,exe ,etc.,)

- Encrypted file is uncrack able (as it is encrypted using AES algorithm) until and unless key is known.

- The Encryption and Decryption process will be very fast using this application

- Providing additional security than AES by encrypting the hexadecimal representation of data.

IV. SCOPE OF APPLICATION

- Companies often possess data files on employees which are confidential, such as medical records, salary records, etc. Employees will feel safer knowing that these files are encrypted and are not accessible to casual inspection by data entry clerks (who may be bribed to obtain information on someone).

- Individuals may share working space with others, of whose honour they are not entirely sure, and may wish to make certain that in their absence no-one will find anything by snooping about in their hard disk.

- A person or company may wish to transport to a distant location a computer which contains sensitive information without being concerned that if the computer is examined en route (e.g. by foreign customs agents) then the information will be revealed.

- Two individuals may wish to correspond by email on matters that they wish to keep private and be sure that no-one else is reading their mail.

- Can be used in small institution such as a small university for lecturers' daily use of sending exam files and sensitive material such that the material can be encrypted and the file is sent in one e-mail while the encryption key is sent in another e-mail or via any secure communication channel.

- Porting this application to different platforms like windows phone , Android , Windows 8 ,etc.,

- Further, providing security to the data while sending an SMS from a phone. The text which is to be sent will be encrypted at source and will

International Journal Of Advanced Research and Innovations Vol.1, Issue .2
ISSN Online: *2319 – 9253*
Print: *2319 – 9245*

be decrypted at destination to get the original text back.

- Providing compression and decompression which decrease encrypted file size and conversion time.

V. IMPLEMENTATIONS

Figure I

The basic user interface of the application is shown in Figure 1.

It allows the user to browse the file which is to be encrypted, the name to be given to the encrypted file.

The buttons “Encrypt”, “Decrypt” and used for encryption and decryption of the file.

Figure 2 shows the browsing of a file using a file dialog.

Figure 3 prompts the user to select the required files before encryption process is started.

Figure 4 promts the user to enter the password and it is internally been converted to 128bit.

Figure 5 gives a pop up saying the user that the task is completed.

Figure II

Figure III

International Journal Of Advanced Research and Innovations Vol.1, Issue .2
ISSN Online: *2319 – 9253*
Print: *2319 – 9245*

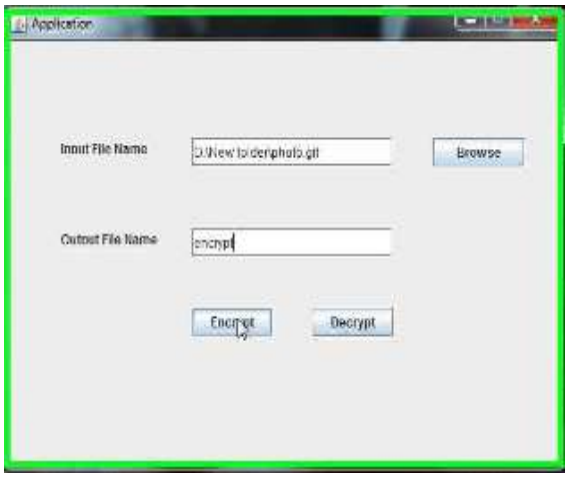


Figure V

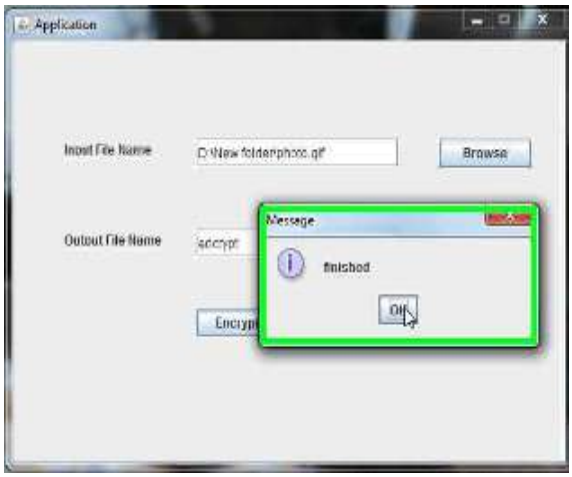
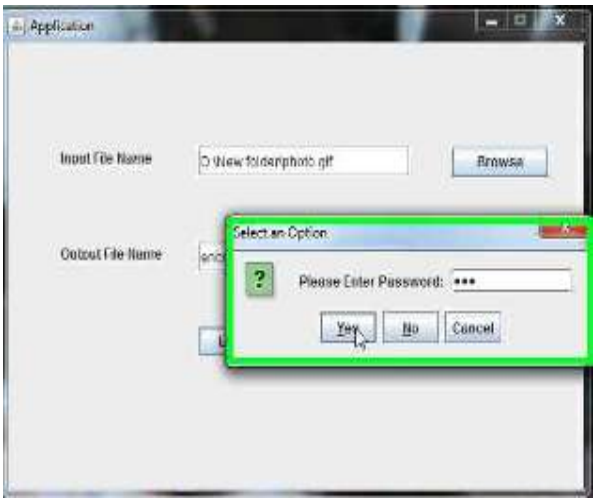


Figure IV



VI. CONCLUSIONS

The version of this application is V1.1. Most of the formatting instructions in this document have been developed and compiled using Eclipse and Java as programming language.

REFERENCES

[1] www.wikipedia.org

[2] www.stackoverflow.com

[3] www.way2java.com

[4] http://docs.oracle.com/