Volume 3, No. 2, March-April 2012
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Any File Encryption by Translating ASCII Value of Characters

Md. Mizanur Rahman
Lecturer, Department of Computer Science & Engineering
Dhaka International University, Bangladesh
mathmasum@gmail.com

Abstract: This paper presents an ASCII based Encryption/Decryption application that is applicable to any type of files; for example: image files, data files, documentation files, audio files, video files etc. It introduces a method of encryption by translating ASCII value of characters of the file opened in binary mode. ASCII value of every character of the file is translated by an integer which is generated irregularly from the key. Size of the encrypted file remains same as original file and required time is also very less.

Keywords: Encryption, Binary mode, ASCII Value, Translation, Decryption.

I. INTRODUCTION

Cryptography is the system where encryption and decryption techniques are used to the network and computer for security of the file. Encryption means the change of original information (plain text) into another form (cipher text) by some operations to make the file unreadable and decryption means the techniques of getting the original information by some operations from the encrypted file [1].

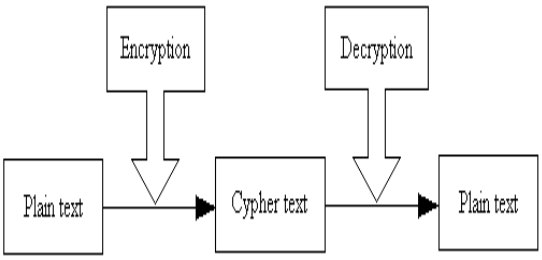

Figure. 1: Cryptography process

Key based algorithms use an encryption key to encrypt a file. There are two general categories for key-based encryption: symmetric encryption which uses a single key to encrypt and decrypt the file and asymmetric encryption which uses two different keys- a public key to encrypt the file and a private key to decrypt it. Currently there are several types of key based encryption algorithms such as: DES, RSA, PGP, Elliptic curve and others but all of these algorithms depend on high mathematical manipulations [2, 3]. Some methods are not suitable for any file [1, 4]. The proposed method will overcome the size problem. Input file and encrypted file are same in size. Required time by this method is also less than the time required by some methods such as zigzag rule, simple encryption/decryption application [4, 5].

II. PROPOSED METHOD

This method is a symmetric encryption and use very simple mathematical calculation. In this method a file is opened in binary mode. ASCII values of characters of the file are translated by integers which are generated irregularly by mathematical sine and ceil functions using the key. Translated characters are written into a second file created in binary mode that is the encrypted file.

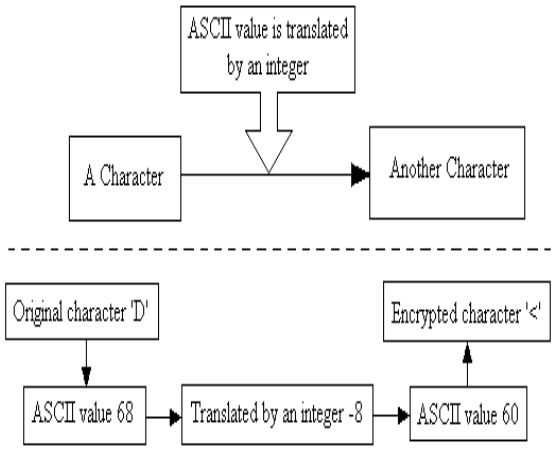

Figure. 2: Character translating with an example

Encryption Flow Chart:

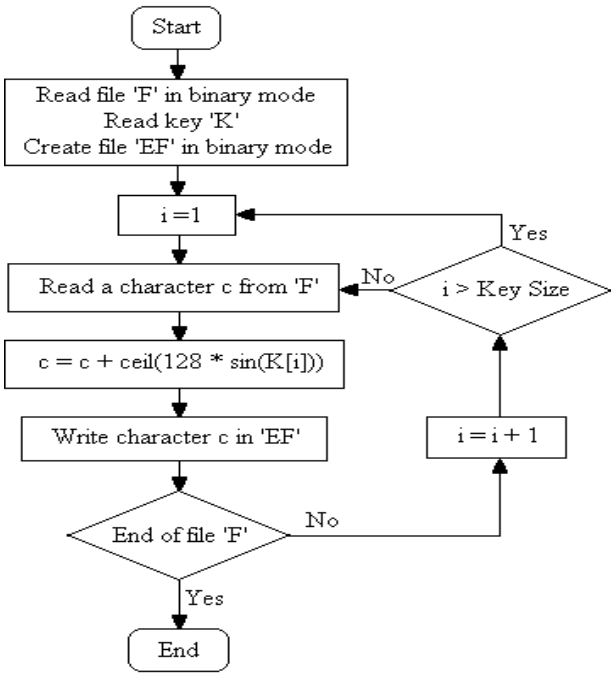

Figure: 3

Decryption flow chart:

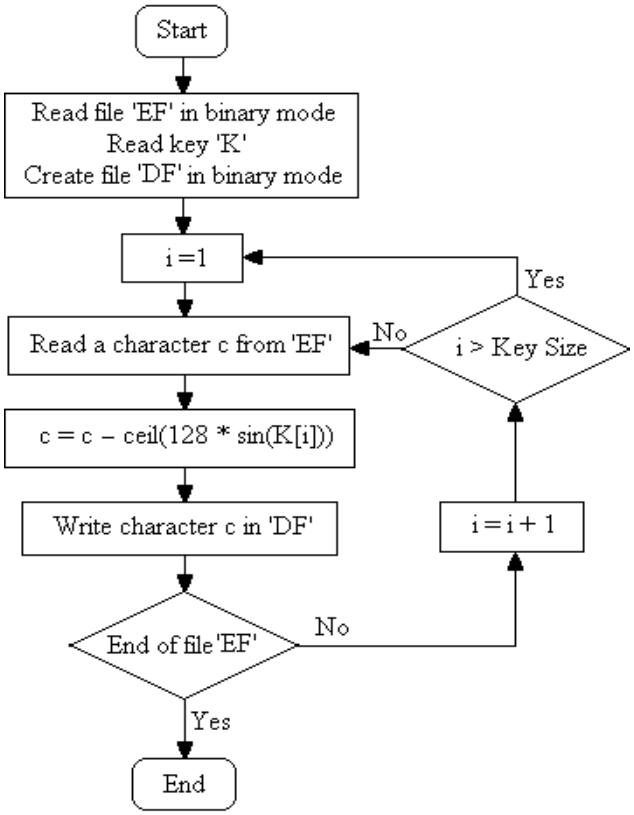

Figure: 4

Illustration:

The following image file sunset.jpg is used to illustrate this method.

Figure: 5

The following image shows when sunset.jpg file is opened with notepad.

Figure: 6

The following image shows when encrypted sunset.jpg file is opened with notepad.

Figure: 7

If we open this encrypted file with ‘Windows Picture and Fax Viewer’ application, then ‘No preview available’ is appeared.

III. PERFORMANCE ANALYSIS

We analyze this method with some files listed below. We have used machine Intel® Pentium® 4 CPU, 3.00 GHz, 504 of RAM. After running the software build in programming language C we get following data. From data (Table-1), it is seen that small amount of time is required to encrypt and the size of encrypted files remain same as before encryption. Required time is also showed by zigzag rule [4].

Table-1: Required time and size of encrypted files

Name	Size Before Encryption (KB)	Time in this method (in second)	Size After Encryption (KB)	Time in zigzag rule (in second)	Ratio: time/KB
Blue hills.jpg	27.8	0.000000	27.8	0.164	0
SUNSET.JPG	69.5	0.000000	69.5	0.549	0
Water lilies.jpg	81.8	0.054945	81.8	0.659	0.000672
WINTER.JPG	103	0.054945	107	0.824	0.000533
Beethoven's Symphony No. 9 (Scherzo).wma	599	0.219780	599	---	0.000367
New Stories (Highway Blues).wma	742	0.274725	742	---	0.00037
a.bmp	1403	0.439560	1403	---	0.000313
As.jpg	2765	0.934066	2765	---	0.000338
Bs.jpg	3308	1.153846	3308	---	0.000349
a.xls	4085	1.428571	4085	---	0.00035
Asdf.pdf	15974	5.329670	15974	---	0.000334

The last column of Table-1 shows that the ratio between required time and size of file is about constant and it is around 0.0003 Second/KB. Therefore, to encrypt a file sized 1 GB, required time is about 5 minutes by a machine Intel® Pentium® 4 CPU, 3.00 GHz, 504 of RAM.

There are 94 visible characters to use in key. If key length is from 1 to 128, then number of possible keys generated is

$$94 + 94^2 + 94^3 + 94^4 + \cdots\cdots\cdots + 94^{128} = \frac{94(94^{128} - 1)}{93} = 3.67 \times 10^{252}$$

If unauthorized anybody tries to decrypt an encrypted file, then there are 3.67×10^{252} possible keys to use. If a wrong key is used to decrypt, then the file will be damaged forever.

IV. CONCLUSION

In this method, simpler but very effective low-level technique is used to encrypt any file. Some files are encrypted by this method. It is showed that very small amount of time is required to encrypt but it is impossible for cryptanalysis. Again, size of encrypted file remains same as original file. By programming language C we can create an encryption/decryption application very easily according to this algorithm.

V. REFERENCES

[1]. Anupam Kumar Bairagi, 2011. ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security, IJCIT, Volume 01, Issue 02, Manuscript code: 110112.

[2]. Beth T. and Gollmann D. 1989. ”Algorithm Engineering for Public Key Algorithms”. IEEE Journal on Selected Areas in Communications; Vol. 7, No. 4 PP. 458-466.

[3]. IBM. 1994.”The Data Encryption Standard (DES) and its strength against attacks”. IBM Journal of Research and Development, Vol. 38, PP. 243-250.

[4]. Saiful Islam, Jahanara Akhtar, Md. Mizanur Rahman, Jinat Sultana, 2009. Image Encryption by Zigzag Rule, Journal of Dhaka International University, Volume 1, No. 1, pp. 150-153.

[5]. Majdi Al-qdah, Lin Yi Hui, Simple Encryption/Decryption Application, International Journal of Computer Science and Security, Volume (1): Issue (1).

