© 2018 IJSRST | Volume 4 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

New Approach for Reducing the Size of Ciphertext

K. Kasikumar*[1], Dr. S. S. Dhenakaran[2]

*[1]M.Phil Scholar, Department of Computer Applications, Alagappa University, Tamil Nadu, India

[2] Professor, Department of Computer Science, Alagappa University Tamil Nadu, India

ABSTRACT

Cryptography is a mathematical logic used to generate secret code for a given confidential input text for maintaining one's own secret or sending them to other intended person over internet. Cryptography basically requires key and encryption algorithm to prepare secret code and decryption algorithm to regenerate the original text from secret code. The encryption algorithm is a program that mixes input text with key values to produce secret code. Here the key value is either generated by random number or prepared by some other means. The mixing of input text and key produces unintelligible code called ciphertext. This ciphertext must be very difficult to understand and reproduce the original text. That is, the ciphertext has to hide the meaning of the input text to maintain the meaning of secret code.. The objective of this work is to create an encryption algorithm to produce secret code for a given input text as well as to reduce the size of the ciphertext / secret code. It is well known that private key / public key mechanism supports secret code writing in cryptography. The proposed work uses private (or secret key) key mechanism to implement the requirement of encryption algorithm. It is understood that a complicated key and a good encryption algorithm are needed to create better secret code and challenging to the hackers to understand the secret code.. Hence the intended work depends on the key construction and encryption algorithm. This paper introduces a new approach to construct the private key and an innovative algorithm doing the job of ciphertext generation. This approach inspects only half of the input text for secret code generation and key generation is done from the input text itself. It is designed to conserve space of storage as well as to reduce time of secret code generation for adding security to the input text. The implementation process deploys input text perplexing, segmentation, key construction and binary operation to meet the intended goal.

Keywords : Ciphertext, Private Key, Text Perplexing, Segmentation, Binary Operation

I. INTRODUCTION

The purpose of cryptography is to protect data in the presence of an adversary. Cryptographic transformation of data is a procedure by which plaintext data is disguised and the resultant is an altered text, called ciphertext, that does not reveal the original input. The ciphertext can be reverse-transformed by a designated recipient so that the original plaintext can be recovered. The transformations are done by private or public key mechanisms.

1.1 Private Key Cryptography

In conventional cryptography also called *symmetric key* cryptography, one key(s) is used both for encryption and decryption. The Data Encryption Standard (DES) is an example of a conventional cryptosystem that is widely employed by the Federal Government of United States[1]. An extremely simple example of conventional cryptography is a substitution cipher. A substitution cipher substitutes one piece of information for another. This is most frequently done by offsetting letters of the alphabet. For example, if the word "SECRET" is encoded using

Caesar's key value of 3, it offsets the alphabet so that the 3rd letter down “D” begins for encoding. Hence, the input ABCDEFGHIJKLMNOPQRSTUVWXYZ is changed to DEFGHIJKLMNOPQRSTU VWXYZABC by sliding each character three positions down. Here the key value is 3. It is the encoded message to be shared with other recipient. Using this principle, the plaintext, "ENJOY" is encrypted as "HQMRB” [1].

1.2 Public key cryptography

Public key cryptography is an asymmetric cryptography where a *pair* of keys is used for encryption and decryption. They are public and private keys where public key encrypts data and a private key decrypts the encoded message to obtain the original text. Here public key is known to others where the private key is kept secret. Anyone with a copy of your public key can then encrypt information that only you can read even people never met. It is computationally infeasible to deduce the private key from the public key. Anyone who has a public key can encrypt information but cannot decrypt it. Only the person who has the corresponding private key can decrypt the information.

II. LITERATURE REVIEW

Informaton security using cryptography is an important science[1].cryptography is an important component of secure information and communucations system. There is always a growing need for protection of information[2]. Cryptography has emerged as the main alternative to protect internet data. The crypto technique mark, transform and reformat the message to protect them from disclosure, change or both, making it safer on transit between computers.

During an encryption/decryption process a large amount of computing resources like CPU time, battery power and memory is consumed from the devices. In some networks like mobile ad hoc networks, there is a constraint on power consumption, so there is a need to improvise the battery technology. So, it is essential to find a way to reduce the consumption of battery powered devices. This algorithm presents a potential solution of energy consumption in various handheld devices using commonly used symmetric key encryption algorithms. [3, 4] It was seen in Triple-DES after 600 encryptions using a 5 MB file the remaining battery power is 45%, which prevents the device from subsequent encryptions.

III. PROPOSED METHODOLOGY

The proposed encryption system is a novice approach to reduce the size of the ciphertext. It is a secret system using two secret keys of same size but one key is operated at a time. The input text to the system is segmented into two halves. First half is considered as actual input to the encryption mechanism and other half is considered as key. The actual input is once again segmented to two halves namely seg1 and seg2. When the size of input text is odd, the odd character at the end of actual input is carried out with seg2 by adding a constant value to generate a cipher code. Similarly, the second half of the input text considered for key is once again divided into two halves namely key1 and key2. Then seg1 and key1 are combined by binary operation taking one character from seg1 and key1 to generate ciphercode C1i . Similarly seg2 and key2 are combined together as before to produce ciphercode C2i. The concatenation of all C1i is called ciphertext C1. The combination of all C2i is called ciphertext C2. The final outcome of the encryption is obtained by the concatenation of C1 and C2[3,4].

The merit of the system is to reduce the size of the ciphertext[2] by half the size of input text. This is useful to save storage size of the ciphertext and the length of the ciphertext may imitate to the hackers to produce some other original input. This anomaly may deceive hackers generating the original text. That is, the resultant is an unintelligent code which cannot be easily reverted to the length of input text Also half of the processing time is reduced by this method. But the key size is increasing when the size of the input increases. Further the key is dynamic which is not same for all types of input. It means, it has different key for different input text since the key is constructed from the input text only. Say for a block of 512 bytes the key size is 128 and for 1024 bytes, the key size is 256 byte. Also, the key value is not a simple a number but it is a core of alphabetic characters. So it is difficult to remember the key value. The sender and receiver must carefully share their secret keys and authentication may be checked by sharing the key two or three times. That is, to check hackers involvement, the ciphertext and key are shared again at different time interval for authorization. The value of C1 and C2 are

C1 = C11+C12+C13+…….C1m

C2 = C21+C22+C23+…….C2m

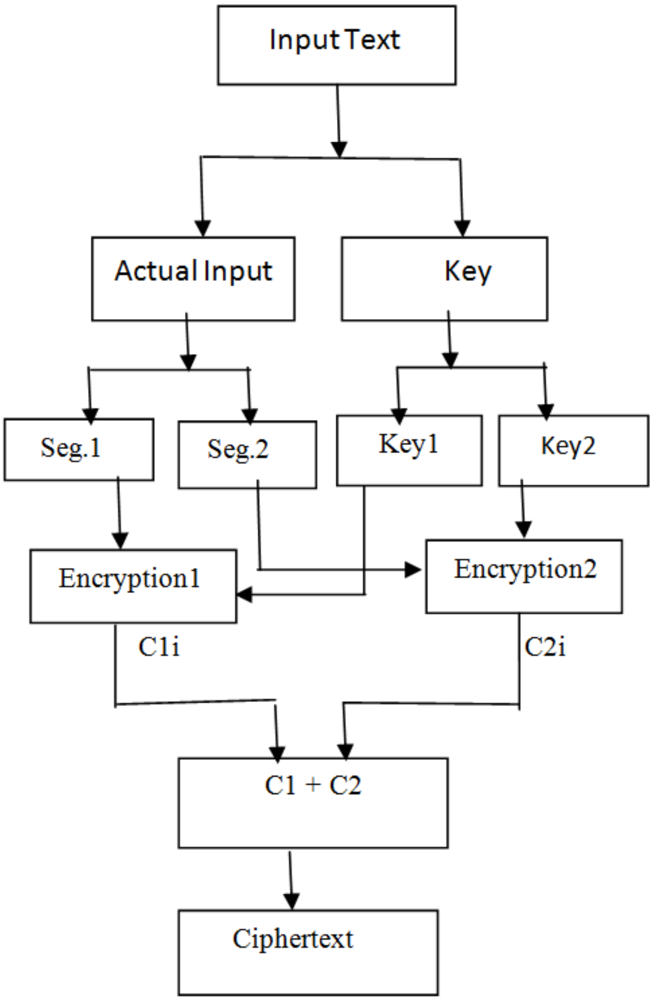

Figure1: Functional Block Diagram

IV. RESULTS AND DISCUSSIONS

The proposed approach is tested by several examples. For simplicity, three samples with their input text and ciphertext are tabulated. In the first example the size of the input text is thirteen and hence the key size is three with three characters of input text. Its cipertext is only seven characters long. In the second example, the size of the input text is ninety two and hence the key size is twenty three and its corresponding ciphertext is fourty six. Similary, the size of input text to the third example is five hundred and seventy and key size is one hundred and fourty two. Its corresponding ciphertext is two hundred and eighty five. The examples clearly show the size of the ciphertext reduced and thereby reducing processing time of encryption. Further the proposed approach is compared with existing AES, DES methods.

TABLE I. EXPERIMENTAL RESULTS

Input Text	Key Size (bytes)	Ciphertext
Alagappa univ	3	±ÑÑÜ×àØ
This is alagappa university which was initiated & founded in 1985 at karaikudi by alagappar.	23	ØãÙ• Ü×àÑåÙÕãä • ØÓ• Ñ• ÞäÑÄÙã ÑÑÑà• ÞæâÙéçÙ ØçãÙÙÙä□˜
Alagappa University is located at Karaikudi in Tamil Nadu is accessible from Madurai and Tiruchirappalli Airports within two hours. The 440 acre green and lush campus houses all the academic activities. This University has emerged from the galaxy of institutions initially founded by the great philanthropist and educationist Dr. RM. Alagappa. Alagappa University was brought into existence by a Special Act of the Government of Tamil Nadu in May 1985 with the objective of fostering research, developmentt and dissemination of knowledge in various branches of learning.	142	¢£O¢›’£“• O• • š“O • ƒœ›}“O¢• ’¢˜›O¡ œ|“¡˜• “ƒ¡’˜• Ÿ›˜p¡ □£O˜—• £□— ¤¢O—OcO’”– ”• • “›¢O• Ÿ¢— ¤”O›O— O’“œ’• £¥£”]ƒ˜O• ¥¡˜¨—¢”‘”– “•□OO• • ¨□O• £££ □¢˜˜˜›¨•¤“““Op• • ŸO• ¥¡˜¨˜O□• ”O£ z¡˜¤˜˜O• ˜O• ¤˜O ’”¢‘”•□O• ¤• O• O˜ ¤— ¡Ÿ• ›O˜Ÿ¡¢¦£˜O¦O □¡]ƒ”c_• ¡O¡”O• O¤ — ’œ¤O□¢¢• ›£”• • ”˜ O’˜˜˜¢O— ¢„˜”¢£O• Oœ¡”O¡ œ£”– ›§O•˜¢˜¤˜• O• £• › O□• ”O¨£O£□¢˜˜]

V. COMPARISON OF RESULTS

Since the objective of the propose d approach is to reduce the size of the ciphertext, the desired system is compared with AES and DES systems. The file size of 570 bytes are considered to test verify the outcome of AES, DES and proposed mechanism. The key sizes of AES, DES are 18. 8 and 142 bytes. Though the size of the key is big in proposed mechanism compared to the other two system, the objective of reducing size of ciphertext is achieved. Also the storage of ciphertext and execution time are reduced. The results are tabulated and pictorially represented in TABLE II and Figure2 respectively.

TABLE II. SIZE OF CIPHERTEXT

Encryption System	Input File Size(byte)	Key (byte)	Encrypted File Size(byte)

AES	570	18	768
DES	570	8	555
Proposed Mechanism	570	142	285

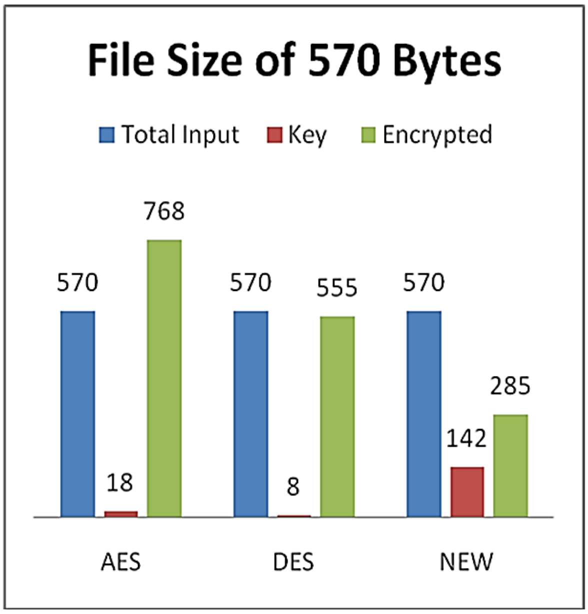

Figure 2: Notion of Ciphertext

VI. CONCLUSION

The proposed approach has implemented with the base of functional diagram principle. The system is verified by a few examples and the results are met the stated goals. Further the objective of the desired work is compared with two familiar methods and the desired work is successful to maintain the size of ciphertext and time of processing. The essential security ingredients of e-business and enterprise computing can be achieved by the proposed work. The integrity and confidentiality can be verified by the size of key regenerated text.

VII. REFERENCES

[1]. William stalings, " Cryptography andNetwork Security Principles and Practices, Fourth Edition ", Prentice Hall, 2005.

[2]. Rolf O, " Contemporary Cryptography", Artech House, Boston,London,2005.

[3]. Network Security: private Communications in a public world, second edition, 2002, c.kaufman, R.perlman, and m. Speciner, prentice-Hall.

[4]. Obaida Mohammad and Awad Al-Hazaimeh, "A NEW APPROACH FOR COMPLEX ENCRYPTING AND DECRYPTING DATA", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.