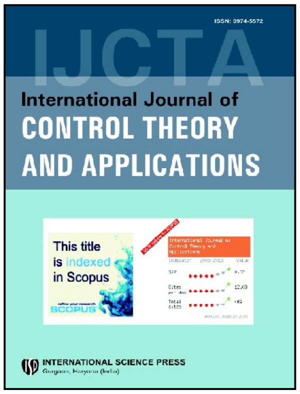

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 11 • 2017

Enhanced Four Stage Encryption

Sangapu Venkata Appaji[1] and Gomatam V S Acharyulu[2]

[1] *Assistant professor, Department of IT, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India, E-mail: appaji_sv@yahoo.co.in*
[2] *Professor(Retd), Department of CSE, Geethanjali College of Engineering and Technology, Hyderabad, Telangana, India E-mail: darsangvs@yahoo.co.in*

***Abstract*:** Though the four stage encryption studied in the previous works well, the permutation of the matrix shuffles the values that are relatively close. There by there is a chance that most of the elements of a block begin with the same alphabet or the most successive letters. The permutation matrix should be able to shuffle the far-end elements, so that the elements in a block have different prefixed strings. This particular point to have far end shuffle is kept in mind and the algorithm is modified to meet the desired condition in this paper. In this paper we proposed a new key which is generated with the K_1 and K_2. This key itself generates the permutation and partitioned sets. The experimental results have shown that no patterns are matched which decrypting with other key, even though a small change in the original key while decrypting there is change in original plaintext. It promises the security against the chosen-plaintext attacks, chosen-cipher text attacks.

***Index Terms*:** Four Stage Encryption, Plain text, Cipher text, Chosen-plain text attacks, Chosen-cipher text attacks

I. INTRODUCTION

Security is important for data communication. A cryptosystem is (M, C, K, e, d) is a quintet. Where M is called original message space or plain text space, C is called cipher text space, K is a key. 'e' is the encryption function and the 'd' is the decryption function. The study of encryption principles is called cryptography. The study of analyzing cipher text without knowledge of key is called cryptanalysis. The study [1-8] of cryptography and cryptanalysis is called cryptology. The definitions of some terms used in cryptography are given by as fallows.

Plaintext: The original data is known as plaintext

Cipher text: The encryption data or un understandable data is called cipher text

Encryption: The process of converting plaintext to cipher text

Decryption: The Process of converting Cipher text to plaintext.

Block cipher: The data is in the form of blocks.

Stream Cipher: The data is in the form of streams.

Key: In cryptography, keys are of two types conventional key or symmetric key or private key and asymmetric key or public key.

Symmetric key: Both sides of sender and receiver use the same key.

Asymmetric key: Two keys one is public key and private key.

Cryptanalysis: The study of cipher text in an attempt to restore the message to plain text.

A. **Types of Cryptography**: Cryptography is classified into two categories as show in fig 1. One is for the symmetric cryptography or private key cryptography another one is asymmetric or public key cryptography.

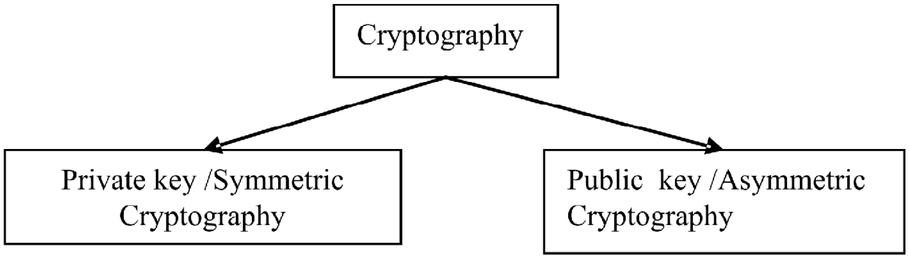
Cryptography
Private key /Symmetric Cryptography
Public key /Asymmetric Cryptography

Figure 1: Types of Cryptography

Symmetric key Cryptography: If the encryption and decryption algorithms are using the same key is called symmetric key cryptography.

Asymmetric key Cryptography: If the encryption and decryption algorithms are using the different keys (i.e. public and private key) is called Asymmetric cryptography.

The four stage encryption is a symmetric algorithm. In the following sections, section II describes the four stage encryption, section III describes the an enhanced four stage encryption, section IV describes the Experimental results and finally section V is describes conculsion.

II. PREVIOUS WORK

In the Four Stage Encryption System (FSE)[9], the input alphabet may be any set, a set of strings of some alphabet or any other symbols or simply the binary set {0, 1}. Unlike in other cryptosystems, the output alphabet in this system is different from input alphabet and generated at run time as strings of input alphabet A of size n. Let α be the plaintext string to be decrypted. Let $K = K_0\ K_1\ K_2$ be the three stage key, K_i is an element of A^+. The output alphabet Z is generated with the help of key K0. The output alphabet set Z is constructed as $Z = \cup a \in A\ a^{\text{index}(Ko(\text{index}(a))}$ and m = |Z| = |A|(å*a*ÎA index(K0(index(*a*)))), where $K_0(i)$ stands for the (i mod |K0|)th letter of K_0. The output alphabet is permuted using a permutation matrix M generated by another key K1. Then with the key K2 a sequence of ‘n’ numbers m_1, m_2 ... m_n, such that $m_{1+}\ m_{2+,}$ ..., + m_n = |Z|= m. First m_1 elements of the permuted alphabet are taken as the set Z_1 , the next m_2 elements are taken as the set $Z_{2,}$ and so on and finally the last m_n elements are taken as set Z_n giving rise to a partition $\{Z_1, Z_2, \ldots Z_n\}$ of Z. Each alphabet of the plain text α is encrypted into a word, the size of which also may vary with each occurrence. The experimental results [9-12] promise the security. While decrypting the procedure of encryption is repeated up to partitioning the output alphabet. The plain text is taken as to be null string. Search for an output alphabet, which is a pre-string of the cipher text. The input alphabet corresponding to the block in which the above output alphabet is concatenated to the plain text. The output alphabet is deleted from the cipher text. The process is repeated until the cipher text is empty.

In The permutation matrix there is a chance of most of the elements of block begin with the same alphabet or at or at the most successive letters. In this paper we proposed a new key is generated with the K_1 and K_2. This key itself generated the permutation and partitioned sets. The main advantage of Four Stage Encryption system lies in adopting a subjective mapping for encryption scheme instead of a bijection.

III. ENHANCED FOUR STAGE ENCRYPTION

The Figure 2 shows an overview of the enhanced four stage encryption. Here we are consider an input set containing an N elements either symbols or letters. The Step1 process creates ‘n’ number of files. Here the Alpha file also contain the same number of elements as input file. Every letter of input file is appended to the alpha file. The result is stored in File1. So, the resultant strings of length two are stored in File 1. Now the input file elements are appended to the File1 and resultant strings length of three are stored in File2. So, the process is continued until the user requirement of the lengths. This process is generated with the first key K_0. In step 2, by applying the key K_1 and K_2 a new key K is generated. Here the key K generates the N number of files whose N is equal to the input set number. Now find the index of first element associated with the key K, by using index of number which file is matched that files string of elements are written one by one to the second step files up to end of the file. Find the index of all key of K and write the corresponding strings into the files in the step2. Finally we obtained the permuted and partitioned sets. Now taking the input file as plaintext and read the first string or element in the file. Look at the first element associated with the string. Find the index of that letter or symbol. Find the associated file number. A random function with respect to the current time and date. The random function selects an element in the file which writes a string in the cipher text file. So, the process is continued until the plaintext file is end. Where the N is considered for any N elements of input alphabet set.

File 1: Appended each element from the input file to the Alpahfile elements and results stored in File1. So, the File consists of strings of length 2.

File 2: Appended each element from the input file to the file1. So the File 2 consists of strings of length three.

File N: Appended each element from the input file to the File (N-1). So the File N consists of strings of length (N+1).

Step 1: Creating the number of files based on the key K_0:

Step 2. All strings in the File1, File2 … File n are permuted and partitioned by using the Key K. and results stored in File 1, File 2… File N, Where K generated from the keys K_1 and K_2.

Step 3: Taking the Input File as Plaintext/ Cipher text file.

Step 4: Do the Encryption/ Decryption Process.

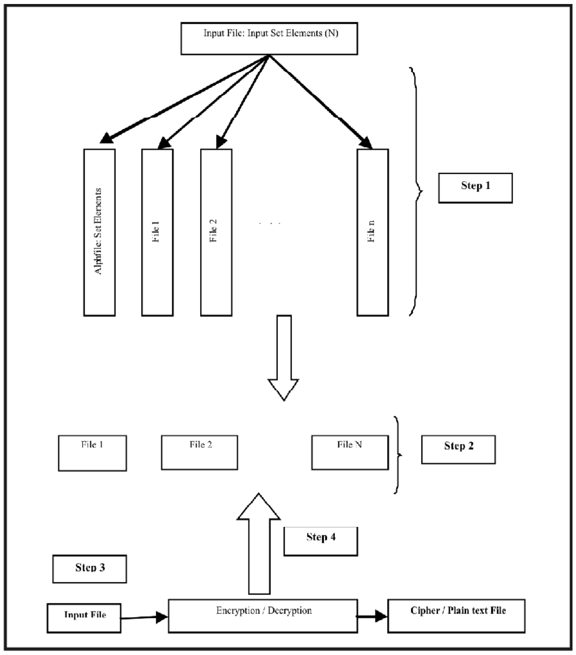

Figure 2: Enhanced Four stage Encryption and Decryption Process

ALGORITHEM: Generating a key that permutes and partitions based on the keys $K_{1,}$ K_2

Input: Giving the Keys K_1, K_2 as input

Output: Generate the a new Key K that will permute and partitioned the Output Alphabet set

```
Begin
Begin
    Initialize the key K with null string
Let $l_1$ be the size of the string $K_1$
If $l_1 \leq N$
Begin
For i varying from 0 to $l_1$-1
Begin
Let ‘ch’ be the $i^{th}$ character in $K_1$
    While ‘ch’ is repeated in K
    ‘ch’← next ‘ch’ ( if the ‘ch’ ‘character is last character next Character is taken to
    be first character of alphabet)
        End while.
End for.
Let K be concatenate the ‘ch’.
For j varying from $l_1$ to N
Begin
Let ‘ch’ be the $j^{th}$ character of $K_1$ where j is i mod $l_1$ ( i % $l_1$)
        While ‘ch’ is repeated in K
    Begin
    Increment ‘ch’ modulo N.
    End while
End for.
Let K be concatenate with ‘ch’.
Let K be concatenate with $K_2$.
Else
For i varying 0 to N
Begin
Let ‘ch’ be the $i^{th}$ character of $K_{1.}$
    While ‘ch’ is repeated in K
    Begin
    Increment ‘ch’ modulo N.
    End while
Connecanate the K with ‘ch’.
    End for.
```

```
ALGORITHEM: Generation of N Partition Sets with K
Input:   K is the key as input.
Output:  K key will permute and partitioned the Output Alphabet set.
    1.   Initialize the strings k fname, and sname with null string.
    2.   Open the file consisting of output alphabet in the read only mode.
    3.   Create the N files in the write only mode which represents the N partitions corresponding to the N elements.
    4.   Read a string's' from the output alphabet.
    5.   While the end of the output file is not reached do
    6.       Begin
    7.       Read the next character from the key.
    8.       Obtained the index of this character.
    9.       Write the string's' in to the file that represents the input alphabet
    10.      Corresponding to the input alphabet.
    11.      End while.
    12.      Close the all output files.
```

The above algorithms are implemented and performed the various experiments with the variation of keys. The experimental results shown in the next section.

IV. EXPERIMENTAL RESULTS: ANALYSIS

The Enhanced four stage encryption(EFSE) is applied with various keys on plain texts.

Let us consider the key as K_0 = abrokenclockisrighttwiceaday, K_1 = konwldgeispower and K_2 = strikewhiletheironishot.The EFSE is applied on given below sample message.

A. Plain Text

many savages at the present day regard their names as vital parts of themselves and therefore take great pains to conceal their real names lest these should give to evil disposed persons a handle by which to injure their owners no singhalese whether man or woman would venture out of the house without a bunch of keys in his hand for without such a talisman he would fear that some devil might take advantage of his weak state to slip into his bod

B. Cipher Text

```
ihtkzilhwdiizbziqtvy ijchwipwraijfbgifchiiyqveipbwtiyetx emuyigtdr icmaeitkjyimkdq
itetmiahzxioftvithamiaengidttdibmhy hxpbikcmcinmnt inaaoipqtcignwvdyluiyezkibbre dtiyigndpimuabiailiikjbu
igzkgewebipjpnihqcwiawzl ilfnvibgzn iquovijxbehphdivhjbigorl izvkqiehkoisyedigxqnigiil iacsoiuqdv
ihobyirzhrijwjcikmggirrkcidqikifripiybvoibcjziagdp iivbhipkhulxum ifkbnijckfihmyvipyofiazggishewizyusinplmiofqb
iqvgwivkgliwgnhibdtu iqmurioazqikjnkizlbpelhn hcqpibyceimojgiqqcwievoe htjmjavh
ityqkifxqmihyxqiurvvipdkaicgkxieokq ipadbiljgnijbltionkaipkst iieqeitbzqigomnixwbj iefhbexptisejribcwhitwbw
nvpliharqjcigibjec iagdeipayfifxoaignlqipqsz isahjipvntiyvfyibckmirkmviqlya ixykmidfjqivowyimpou iqogtioghl
iepfkihwtvijyzcijjpj dbgbiocffidaroioucaiayvjietmgihsjhircjv ddxzigddddjevirqfkixetfiijxvigsry ibjdy
ipgpnioathiqrooikgunimpdqicohq hkfciprfn dlycekutiextyilggticoqg ihbwyigtfy hdemipnbkiedbkivloeidzlyipfow
dkjyiadzfidcdpieqhviuvix iknhqibkqtibgraiawwbikxdxihlrc ehbfitmja
ikroyindqxebvgizppsioihwhzzxincsbihnhrkhlmilxai idcbqiewdsialmeinbgwidrmvipexpizptu iwbhbiebgjichrs hefsdcqs
dzgwijjnkigfsfixmgmiiosf igvcjiqkzfiazqwibjieeibu iaclwildiaiuubiidtfiivonlixmfhickdq jcwkiqbqwibtli keoiiuqfs
etgvigcgkimyom igwzpilsmfisssxiynkeicclt itejtikmdeidbsthmeiiydcuemwqimdtv dgvv jqedixtffiepjaibwfgilpwz
```

iocytilnkr ipbzaidybtijuonizrcw hqwwiynes ioaruhdjjhsws iqsukijjzniaygdiicxm ipqcviidewisqvu hocbigeboifbvcipaqzieycyicwfohajs jbsaixajfjungicral ifvzy itkfvikxueimzekidpppiwgdsdjhqiedwfietaw iawkqiskfx iihxkiijqliucrrigedmihvfs idoauigqdeiutlfjidc drwvievqnilzpwdbvo iijsuiucsuidgozifutf izibrijzpxiojjliafwuijdwm egsjimfkwiagqreentiqmoh idqpmihyhnhnboimsts ihebseerfinnkkiekchkljliqdmiiddrwifkvcdzwu idatijtxn iqsqyieelniarhh ihocxdvjbjmkcjohj iwnuihycriflmretkziqgzg iquakiiphg iynnyihuwfikuroihxba ieudsiadqxirouxizyus ibyojefenijhpl hwpjhhtsifsbn

Decryption with the same key: The cipher text obtained in the above is decrypted with same key then the original message is obtained.

Decryption with the small variation in key: Let us decrypt the above cipher text **B** using same K_0 = abrokenclockisrighttwic eaday and left the one letter in K_1 as nowledgeinpower and K_2 = strikewhiletheironishot. The plain text after the decryption is given below.

uaoj sakafes at the qresent gaj refarg their oaues as kitae qatts oi trdupeekdp aog thdreiore takd freat qains to cwoceae their rdal oauep eest thepe shwmeg fike yo dkse gisqoseg qersons a hangld bj whsch yo iovmre yrdsr oloerp ow sinfhalese lhethet uan wr wwuan womlg keotmre wmy wi the homse liyhwmt a bmocr oi nejs io hsp hang iwt lithomt smch a taeisuan hd lomlg idar thay poud gdkie uifrt tane agkaotafd oi his leak syate to seiq snto hss bog

Even though a small change in the key there is lot of difference in decrypted text.

Let us decrypt the above cipher text **B** using same K_0 = abrokenclockisrighttwiceaday and change in one letter in K_1 as knowledgeinpowe and K_2 = strikewhiletheironishot.

ranu sajages at the present dau regard their nares as jital pamts of therseljes and therefore take great pains to conceal their real nares lest these shoyld gije to ejil disposed persons a handle bu which to invyre their owners no singhalese whethem ran or woran woyld jentyre oyt of the hoyse withoyt a bynch of keus in his hand fom withoyt sych a talisran he woyld fear that sore dejil right take adjantage of his weak state to slip into his bod

Even though a small change in the key there is lot of difference in decrypted text.

Encryption with Interchange of Keys: When K_0 key kept unchanged and K_1 and K_2 keys are interchanged the plain text after the decryption is given below.

pbve mlyrsui op wks qnveaty rog yqhoyw wudlo apbcg lg nwglw qrvlg kv ehelokuege bsw leghjjeot eple zyspr wrlsk wz qljdcld ridrn wepi wlppf wjke yijfv idrkwy oeyf ig knrd ntfdxfeg wtnohvkl ubjrne ce diowm cm ajsdwd oiglr oeawgo wl cpasfpzucc cfaywia ppa on qobrv uednw yqjydgk okf ra geo exwov peimoql p pwsdi et oeef wa kbf opty vra iwydeqy cdqg o bodxmopj ke ogdne jmls biof fmle nxgaq lsihb yloc lgelwylnm nw dvi ppll fplpd lo fwyk rwge dbx

In the above decryption, even though keys are interchanged there is lot of difference in decrypted text.

Decryption with different of Keys: When K_0 key kept unchanged and K_1 and K_2 (K_1 = shewenttouk and K_2 = hewenttousa) are entirely different keys then the decrypted text is given below.

ihrk ccwfnss ot hat lyshdsn ecb hpsstr raejv jehnf rt blifa fhtkb tt motupcegtp wtr uvttpwswx owth adjeq zioeh es nolwbmr tceol swhn hbrqe xtim nhang sheozl wawe vq vgrw wthaentu ozetadu q oobcoa bt nbmsb tw ouueqa unpow peoeqz sy rizegotyah esneagu fnd gq nychw enoad thtvwtc ktj tt uak yhucn ehnbhjg u ohese cc bwnl rw trw uowb sej amqmsuw uyhv i cszyfhnn hm taeat hsti tdar nlqi xzern ecmss lvti wpzhmuess sr als xkis dmxfw jr vaxj jaos oek ssg

Encryption with the same key in second time: If second time if you use the same keys and encrypted then the cipher text is different, because we are using random replacements in the partition files. So, every encryption produces different cipher texts with the same key.

V. CONCLUSION

The examples of results show that even though there is a small change in the keys it is difficult to retrieve the original text from the cipher text. Even if the user tries to encrypt the text several times then different cipher text will be produced. So, the enhanced four stage encryption is efficient against the chosen cipher text and plain text attacks. The permutation of elements are faraway due to the new key. In case of four stage encryption we are using three keys, But here in enhanced four stage encryption by using second and third key generating the new key. This key is used for permutation and partition of the elements in a far away. Here generating the new key using second and third key.

REFERENCES

[1] C.E. Shannon, “A Mathematical Theory of Communication”, Bell System Technical Journal, vol. 27, pp. 379–423, 623-656, July, October, 1948.

[2] Shannon, Claude. “Communication Theory of Secrecy Systems”, Bell System Technical Journal, vol. 28(4), page 656–715, 1949.

[3] Massey, J.L, “An Introduction to Contemporary Cryptology”, Proceedings of the IEEE, Special Section on Cryptography, 533-549, May 1988.

[4] Meyer, C.H. Cryptography-a state of the art review Volume , Issue 8-12 May 989 Page(s): 4/150 - 4/154.

[5] J. Hoffstein, J. Jipher, J. H. Silverman, “Introduction to Cryptography in Mathematical Cryptography,” Springer-Verlag, 2008, pp. 38.

[6] X. Lai and J. Massey. A proposal for a new block encryption standard. In Proceedings of the EUROCRYPT 90 Conference, pp. 389-404, 1990.

[7] S. Hebert, “A Brief History of Cryptography”, an article available at http://cybercrimes.net /aindex.html.

[8] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[9] Gomatam V S Acharyulu, Sangapu V Appaji, “ Four Stage Encryption,” International Journal of Research in Computer and Communication Technology, Vol. 1, Issue 4, pp. 129-132, Sep. 2012.

[10] Gomatam V S Acharyulu, Sangapu V Appaji, “Analysis of Four Stage Encryption,” International Journal of Research in Computer and Communication Technology, Vol. 1, Issue 6, Nov. 2012, pp. 338-339.

[11] Sangapu Venkata Appaji, Dr.Gomatam V S Achrayulu, “Four Stage Encryption Generalizations: Partitioned output Crypto System,” International Journal of Computer Applications (0975 – 8887),Volume 108 – No 17, December 2014, pp:26-23.

[12] Sangapu Venkata Appaji, Dr.Gomatam V S Acharyulu, “ A Study Of four Stage Encryption: Experimental Results.” 2014 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Park Engineering College, Coimbatore, Dec, 18-20, 2014.