RESEARCH ARTICLE OPEN ACCESS

New Technique Using Multiple Symmetric keys for Multilevel Encryption

Dr.Yasir Khalil Ibrahim
Jerash University

ABSTRACT
In a world of **accelerating** communications, cryptography has become an essential component of the modern means of communication systems. The emergence of the webas a reliable medium for commerce and communication has made cryptography an essential component. Many algorithms or ciphers are in use nowadays. The quality of the cipher is judged byits ability to prevent an unrelated party fromknowingthe original content of the encrypted message. The proposed "Multilevel Encryption Model" is a cryptosystem that adopts the basic principles of cryptography. It uses five symmetric keys (multiple)
in floating point numbers, plaintext, substitution techniques and key combinations with unintelligible
sequence to produce the ciphertext. The decryption process is also designed to reproduce the plaintext.
Key Words: Cryptography, symmetric key, ciphers, algorithms, plaintext, encryption, communication systems

I. INTRODUCTION

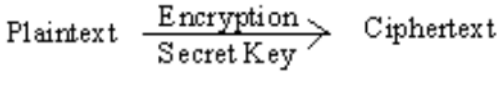
With the enlargement of the net andalso the growth electronic commerce, cryptography has become crucial to business group action andlegal exchange. This information should beprotected from unauthorized eyes. To achieve this goal, cryptography is thetechnique used to protect data. Cryptographycan be divided into two branches, known as transposition and substitution.Two major areas of Cryptographic architectureexist. They are symmetric keycryptographyand public key cryptography. The symmetric key based algorithms are called conventional cryptographic algorithms. They are implemented usingtwo types of ciphers called "block ciphers" or "streamciphers". Stream ciphers can encrypt a single bit of plaintext at a time, whereas block cipherstake a number of bits and encrypt them as a single unit. Stream ciphers are used more dominantlythan block ciphers, as the chunkis encrypted bit-by-bit basis. This process is much smaller and faster than encrypting large chunks or block of data. This method uses a secret key whichis shared by both sender and receiverof themessage. The symmetric key has five basic elements. It requires a strong encryption algorithm and the sender and receiver
must have copies ofthe secret key in asecured form. We define the encryption and decryption process of
the symmetric system (see figure 1 &2) by the following relationship. Let M be the message and K be the keyand E be the encryption function.Then the cipher text of thecryptosystemis given by

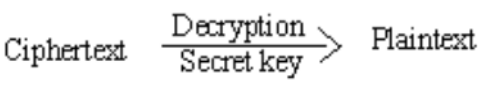
$$C = E(K, M) \quad \text{.....(1)}$$

The decryptionprocess of obtaining the original
message / plaintextis given by

$$M = D(K, C) \quad \text{.....(2)}$$

A description of symmetric key system are
described as follows





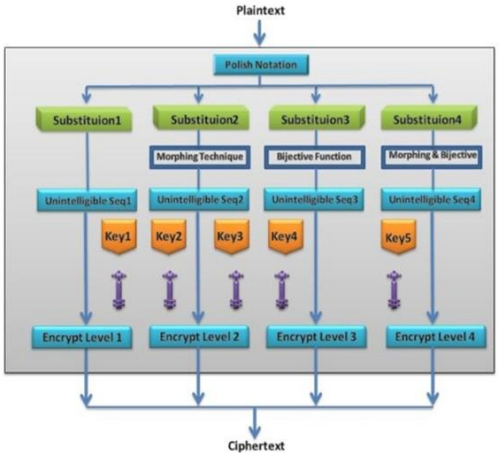


Figure 1 Proposed Encryption System

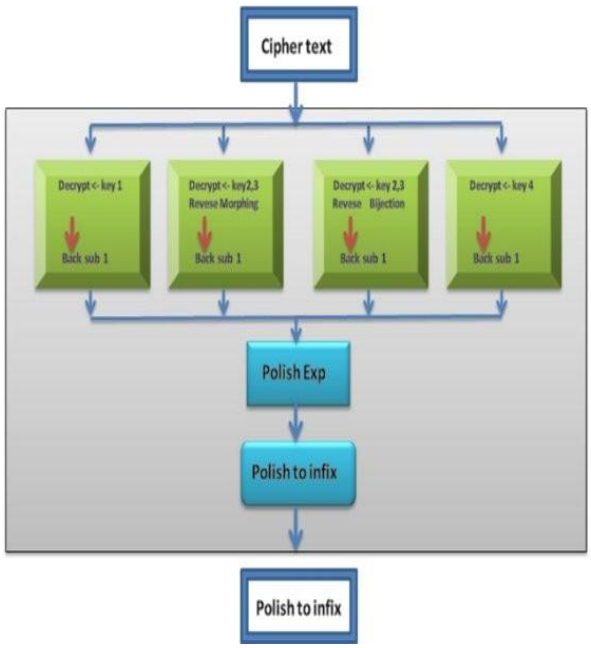


Figure 2 Proposed Decryption System

paper, we will discuss a proposedalgorithm which is uses 5 keys in theprocess of text encryption. THE PROPOSEDALGORITHM The proposed method
is a novice method that works on mathematical principles via polish representation of mathematical
expression, morphing technique and bijective functions. It is a block cipher employing 128 bits key that operates on64 bit data block. We use the
same procedure proposed by [6] but with modifications onthe number of data sets andthe number of floating point keys.

THE PROPOSEDALGORITHM

The proposed method is a novice method that works on mathematical principles via polish representation of mathematical expression, morphing technique and bijective functions. It is a blockcipher employing 128 bits key that operates on 64 bits data block. We use the same procedure proposed by [6] but with modifications onthe number of data sets and number of floating point keys.

MENAEncryption Algorithm

Ciphertext (Plaintext [], int d1, d2, d3, d4)

Begin

Problem Specification:

Modern computers and communication systems use many electronic devices to exchange data over high speed communication lines. The communication systems also take care of data before passing them over transmission lines. Manymathematical methods are used tosecure data [2].To avoid intruders from hacking information, cryptographic principles are introduced. The goal of the proposed method is to transfigure the message that can't be easily identified except by the respondent [1]. It is intended to introduce multiple symmetric keys to furnish multilevel encryption [3].The keys are obtained fromthe contents of user's personal information andthe digital signature[4].T o effectively usethese multiple symmetric keys, the given message is mangled using mathematical logic and then it is divided into pieces[4].Then some computing functionss are generated and applied to
these pieces to yield a better unintelligible sequence. Appropriate key(s) are operated or applied on the
unintelligible sequence to generate theciphertext.

Objective and Scopeof the Research:

The prime objective of this research is toformulate a new crypto modelto succeed with multi level
encryption [5]. The proposed crypto method is built with mathematical logic for key generation, tree traversal technique, and suitable substitution with
morphing principles and bijective functions. The research proceedsin more than one phase, but in this

```
Read Plaintext
        Call polish notation to obscurethe
plaintext
          Segmentthe resultantinto dataset1,
dataset2, dataset3,dataset4,
sizes d1, d2, d3,d4, partial codes
for round = 1 step1 to d1 subbytes (dataset1)
endfor
for round = 1 step1 to d2 subbytes(dataset2)
            Apply dilation to expand the
partial codes to get intermediate code
endfor

for round = 1 step 1to d3 subbytes(dataset3)
Apply bijection to create new imagefor
partial codes endfor
for round = 1 step1 to d4
  subbytes (dataset4) Apply

endfor

for round = 1 step1 to d1
for shift = 1 step 1to subbytes value rotate
left(Key1)
endfor

Ciphertext*/

endfor j = 0
c = 0
ciphertext1← result /*First Level display

ciphertext1

ciphertext */
j = j+1
if j > 2 set j = 0 ;
c = c+1
if c > d2 break ;
for shift =1 step 1 to subytevalue j rotateleft
(Key3)
endfor
          ciphertext2←result /* Second
level ciphertext*/
display ciphertext2
endfor

          for round = 1 step 1 to d3
for shift = 1 step1 to subytevalue rotate left (Key4)

endfor
        ciphertext3← result /* Thirdlevel
ciphertext*/
```

The proposed method is a block cipher employing
128 bits keys that operate on 64 bits data block. It uses five floating point keys of 128 bit size. The
efficiency of the proposed method is tested with P4
3GHz machine. The encryption and decryption times are tabulated taking files with different

```
for round = 1 step1 to d2 c = c+1
          if c > d2 break ;
              j = j+1
           if j > 2 set j = 0
             for shift = 1 step 1to
subytevalue j
rotate left (Key 2)
endfor
ciphertext2← result  /* Second Level
```

contents and different sizes. It is noted that the tabulation did notinclude keycalculation time (see Table 1). As per theresults obtained, methodshows better performance over other algorithms such as AES.The performanceof the proposedsystem is shown graphically(Figure 3). Also the results are compared with otherthree existingmethods.

Table 1 Computational Time of Various Methods

Input size (bytes)	DES 56-bit key	AES128-bit key	BF 64-bit key	MENA 128-bit key
600	0.06	0.108	0.06	0.084
1350	0.14	0.24	0.14	0.19
2100	0.22	0.32	0.21	0.3
2680	0.28	0.5	0.27	0.42
5200	0.5	1.0	0.5	0.75
10000	1.1	1.65	0.82	1.43
12000	1.31	2.1	1.05	1.68

It is clearly notedfrom the above table that our method gives better results compared with AES, but the same results showsthat MENA computational time is a bit more than that of DES and BEF,the reason behind thatis the presence ofmultiple floating point keys,computational functions and variable number of key rotations.

```
display ciphertext3
endfor
```

j = j+2
if j > 3 set j = 0 ;
c = c+2
if c > d4 break ;
for shift = 1 step 1to subytevalue j rotateleft (Key5)
endfor
ciphertext4← result /*Fourth level ciphertext*/
display ciphertext4 endfor

Results & Discussion

Figure3 Graphical Comparisonof DES, AES,BF and MENA

The proposed method is a64 bits blockcipher employing 128 bit keys. It uses five floating point symmetric keys of 128 bits size.The symmetric keys are the solution of two real valued functional equations.These computing function are put together to build unintelligible sequence in the proposed system.

Then, unintelligible sequence1 is combined with key1 to yield first level ciphertext, key2 and key3 are combined with unintelligible sequence2 togive the second level ciphertext and key4,key5 are combined with unintelligible sequence3 to produce third level ciphertext.As the keys are floating points in nature, the cipher text generatedare lengthycodes which take threefourth of additional space to store the ciphertext.The memory utilization considerably reduced by using"XCQ" technique[7, 8]for compression onthe ciphertext.

Acknowledgment:
The author would like to express nhos gratitude for the University of Jerash for supporting this research

REFERENCES:

[1] [1] Xuejia Lai andJames L.Massey , "A proposal for new block encryption standard" , Advances in Cryptology-Eurocrypt 90 Proceedings, Springer Verlag, Berlin , pp. 389-404, 1991.
[2] [2] Xuejia Lai, "Onthe Design and Security of Block Ciphers", ETH Series in Information Processing 1, Hartung-Gorre Verlag, 1992.
[3] [3] Impagliazzo R and KapronB.M, "Logics for reasoning about cryptographic construction", Proceedings 44 IEEE Symposium on foundations ofcomputer science, pp372-381, 2003.
[4] Kiefer K, "A new design concept for building secure block ciphers", In Proceeding of International Conference on the Theory and Applications of Cryptology, PRAGOCRYPT 96, Prague, Czech Republic, pp 30-41, 1996
[5] Black J. and Rogaway P., "CBC MACs for Arbitrary-Length , The Three Keys Constructions" , In Proceedings of Advancesin Cryptology– Crypto 2000, LNCS 1880, Springer-Verlag London, 2000.
[6] Dhenakaran S.S, Naganathan E.R, "A
[7] New Approach to Multiple Symmetric Keys, IJCSNS VOL.7No.6, June 2007, pp254-259. [7]Vijay S Gulhane, Dr. Mir SadiqueAli , Survey over Adaptive Compression Techniques, IJESIT, Volume 2, Issue 1, January 2013
[8] Wilfred Ng · Wai-YeungLam Peter T. Wood · Mark Levene —XCQ: A queriable XML compression systemKnowlInfSyst (2006) DOI10.1007/s10115-006-0012-z