SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC Transactions on Networks and Communications

VOLUME 2, ISSUE 5
ISSN: 2054 - 7420

# N-Cryptographic Multilevel Algorithm for Effective Information Security

**Olawale S. Adebayo[a], [b]Morufu Olalere, [c]Amit. Mishra, [d]M. A. Mabayoje and [e]Joel N. Ugwu**
[a,b,e] *Cyber Security Science, School of Information and Communication Technology, Federal University of Technology, Minna, Niger State, Nigeria, [c]IBB University, Lapai*
waleadebayo@futminnna.edu.ng; lerejide@futminna.edu.ng; joeljupiter@yahoo.com

## ABSTRACT

Security of information cannot be perfectly realized as both it and its counter technology continue to evolve. In the same vein, using a single cryptographic cipher to realize information secrecy is not enough as it can be broken over time, thus revealing the information in plaintext. Most of the existing cryptographic ciphers possess a minimal level of weakness, which is exploitable over time, but when this algorithmic transformation is used in multiple times, the number of trials, effort, and time required to exploit it become greater. This paper proposes a multilevel algorithm for realizing the security of information using a multiple-cryptographic ciphers process. It presents the possibility of combining n-cryptographic ciphers in a single implementation within the system, permitting n-cryptographic transformation to take place during the encryption and decryption processes.

**Keywords**— Encryption, Cryptography, n-cryptographic algorithms, Cryptanalysis, Multilevel Algorithm

## 1 Introduction

The knowledge of cryptography is evolving. Different cryptosystems have been formulated, and people can now make choices of their implementations ranging from symmetric keys to asymmetric ones. The choice depends on the application of the system. However, the knowledge of cryptanalysis has made realizing perfect secrecy a difficult task; people can now make trials of several keys on a particular cipher in order to decrypt encrypted information. The more stringent an algorithm is, the more effort and time required to realize its encrypted information in plaintext. Such efforts can now be automated, thereby reducing the total time of trial to the nearest minimum. As cryptologists continue to discover more algorithms that will ensure better security and frustrate the existing hacking software; hackers continue to rediscover a means of beating the new ones by developing new systems that can combat the new algorithm.

In the past, scientists have found it difficult to ensure an individual can communicate thought, ideas, knowledge, etc. to another without unintended individuals also having access. This difficulty has resulted in many research projects in the area of information security and secrecy, even before the development of electronic computers. The search could be traced back to early 2000BC when hieroglyphics were used in Egypt to decorate tombs to stylistically tell the life history of the deceased [3]. This area of research was given a name Cryptography, which derives from two (2) Greek words: "Cryptos" and "Graphein" which means hidden or secret and writing respectively. Combining the two,

**DOI:** 10.14738/tnc.25.504
**Publication Date:** 16rd October, 2014
**URL:** http://dx.doi.org/10.14738/tnc.25.504

the meaning now becomes “secret writing or hidden writing”. Cryptology could be seen as a practice and study of techniques for secure communication in the presence of third parties [4, 8].

Cryptography in modern days has evolved through many developmental stages, and several cryptographic ciphers have emerged as a result. Each cipher has a distinct algorithm or emerging from the existing one as a higher specification of the existing one. As these ciphers emerge, hackers also undertake research on how to make the efforts worthless, and so on, making this area a research oriented field [4].

Cryptographic algorithms are essential in securing documents on the communication network [14]. The use of multiple algorithms to realize information secrecy enhances the security of the information by requiring several keys before the meaning of information can be revealed in plaintext. Each of the transformations requires a given level, where each level is assigned 1 (one) and the total level for the transformation is given as n, for both encryption and decryption processes respectively. Take for instance, if the total transformation for a given implementation is two, then n is equal to ‘2’. This paper proposes a generalized algorithm for using more than one transformation cipher on a single plaintext to realize one output. This is termed multilevel cryptography.

## 2 Related work

Lein Harn and Hung-Yu Lin [5] 1990 proposed a key generation scheme for multilevel data security using bottom-up approach. The term multilevel was used to mean variable securities at different access levels with many users of a single system having different keys at each different access level. This approach was formed modifying the approach proposed by Akl and Taylor [10] 1982 using a top-down model. Usha et al. [13] proposed a multilevel encryption-decryption of text into cipher data in which its characters are encoded uniquely into its corresponding cipher and eliminating the possibility of any pattern as described in their paper titled ‘Secure Multilevel cryptography Using Graceful Codes’. It uses more than one level of security by employing many ciphers to disguise any pattern.

Rashmi et al. [9] introduced the culture of securing images using chaotic mapping and elliptic curve cryptography in a network environment. The dependency of stream ciphers on pseudo-stochastic sequences was noted as it can produce a pseudo-random sequence with good randomness. Hardjono and Sebbery [12] discovered a system that makes use of hierarchical keys used to encrypt and decrypt data stored in databases using the RSA cryptosystem with additional restriction of encrypted information to the public. The base of the systems security is discrete logarithms and the term ‘multilevel’ used in this context means multiple users with different securities.

Multi-Level Crypto Disk: A secondary Storage with Improved Performance was introduced by Chaitanya et al, [11]. They discussed the issue of hard disks becoming increasingly vulnerable to security attacks as they are now accessed remotely, either with mobile devices or in other unanticipated operating environments. They highlighted the demerits of using single data encryption on storage devices, proposing a secure disk using multiple crypto levels.

Multi-Level Cryptographic Functions for the Functionalities of Open Database System was designed and implemented by Adio et al. [1]. This is a secure open database system for an organization that can open their information system for access by different users. The implementation does not require input to be hidden from anyone or converted to place holder characters for security reasons, but the user only needs to study the sequence of codes and active boxes that describe his password and uses it in place of his active boxes.

A secure information transmission using Multilevel Steganography and Dynamic Cryptography was proposed by Navneet S. Sikarwar [7] in his paper titled 'An Integrated Synchronized Protocol for Secure Information Transmission derived from Multilevel Steganography and Dynamic cryptography'. He juxtaposed the use of both simple steganography and cryptography proposing that multiple and dynamic codes give more security. Maruti et al. [6] presents a practical implementation of a quasigroup based multilevel encryption for data and speech. It makes use of an indexed scrambling transformation for signal authentication, encryption, and broadcasting applications in secrete-key cryptography. The results presented shows that a quasigroup transformation is very effective in destroying the structure of the input signal, and hence can be a good encryption technique.

# 3 Types of Multilevel Techniques

The major elements of multilevel cryptography are the contributing cryptographic ciphers, which are arranged in a desired sequential order. The term "multilevel" implies that more than one transformation must take place within the system in order to produce an output (cyphertext). The product of a multilevel algorithm is obtained from an organized sequential transformation of input (plaintext) with a desired encryption cipher(s). There are three general classes of algorithms used in multilevel cryptosystems:

a) Same cipher with same key
b) Same cipher with different keys
c) Different ciphers

## 3.1 Same Cipher with Same Key (SCSK)

When a multilevel cryptosystem is made of the same cipher with the same key, the transformation used can said to be an iteration of a particular cipher. The security of the ciphertext now lies on the complexity of the cipher, key management, and the number of the iterations made. Given that the transformation order number of a multilevel cryptosystem with the same key is **n**, then the reverse computations that can be done with the ciphertext in order to regain the message in clear text is also **n**. As the security of SCSK-multilevel implementation lies on the complexity of the cipher, key management, and the number of iterations made, it is quite certain that the owner of the system need to secure their implementation by hiding the cipher used, the key used and the number of transformation made from the knowledge of adversaries.

## 3.2 Same Cipher with Different Keys (SCDK)

A SCDK-multilevel structure is said to have been made when the same cipher is used with different keys at different stages. It is similar to SCSK but uses variable keys per iteration. The keys are varied sequentially based on choice, and are kept constant per given implementation. The security of the SCDK-multilevel structure lies on the type of cipher used, number of keys used, key management, and number of iterations made. The sequential order of keys applied per iteration in the SCDK-multilevel structure should be noted, as it has to be reversed during the decryption process.

### 3.3 Different Ciphers (DC)

When a multilevel technique is enforced with different algorithm, the security of the implementation is high and relies on the complexity of the contributing ciphers, the number of keys used, key management, as well as the number of transformations made. In this case one particular cipher is not used sequentially twice, but can be used after another cipher has been applied, this means that a particular cipher cannot be used for both i-operation and i+1-operation, but can still be used after i+1-operation. This type still has some other subtypes that are determined by the keys used but will not be captured in the general algorithm. The sequential order of encrypting ciphers with their keys should be kept constant as it has to be reversed during the decryption process per every implementation.

## 4 Methodology

Formal method was adopted to define and formalize the definition of n-cryptographic algorithm. A plaintext was designated as input for the algorithm, while the output is the cyphertext. The transformation of cipher ($\alpha i$) and key ($\beta i$) was done using the initial element i. The formal definition of n-cryptographic cryptosystem is done in the following subsections.

### 4.1 Order Number of a Multilevel Scheme (n)

The order number of a multilevel implementation (**n**) could be defined as the number of transformations that will take place before producing the desired output (ciphertext). This number of times does not depend on the type of cipher nor upon the key used. For every implementation, '**n**' is placed as the finite-transform-number, while '**i**' is a variable that an increment as the transformation proceeds. For every transformation, the **i**th value increases with **+1,** while it is set to 0 (zero), at the beginning of an operation. The **i**th value defines the termination of the process given that the transformation rules were kept constant.

The termination of the transformation process is said to occur when the **i**th value equals the value of **n.** hence

*For the first transformation,* $i_1 = 1$,
*For the second transformation,* $i_2 = i_1 + 1 = 2$,
*For the third transformation,* $i_3 = i_2 + 1 = 3$,
. . .
*For the last transformation,* $i_n = i_{n-1} + i_1 = n$.
In a multilevel process, the value of **i** in an uninitiated transform state is **0** (zero), and increments as above.

### 4.2 N-Cryptographic Algorithm for Multilevel Structure

This concept is made to harmonize the general representation of multilevel cryptographic scheme; the implementation adopted several terminologies in order to describe its structure. Such terminologies are explained below:

i. $i$ is an incremental variable that determines the present order of operation
ii. $n$ is the order number of the multilevel structure
iii. $\alpha_i$ is the cipher used per i-operation

iv. ***$\alpha_{i+1}$*** is the next cipher to use after i-operation

v. ***$\beta_i$*** is the key used per i-operation

vi. ***$\beta_{i+1}$*** is the next key to use after i-operation

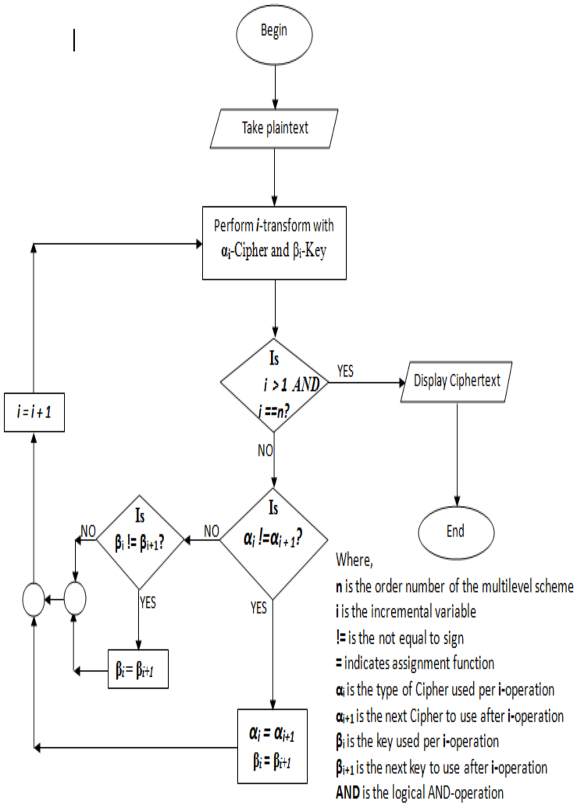
vii. **=** is the assignment operator

viii. ***!=*** is the non-equal-to operator

The n-cryptographic algorithm for multilevel techniques is shown below, and the algorithm is presented in Figure 1:

Table 3.1 Steps in Generalized Multilevel Scheme

| | | | |
|---|---|---|---|
| *1* | *Begin* | *9* | *$\beta_i = \beta_{i+1}; \alpha_i = \alpha_i + 1$* |
| *2* | *Take Plaintext* | *10* | *Else if ($\beta_i$ != $\beta_{i+1}$)* |
| *3* | *Perform i-transform with $\alpha_i$-Cipher and $\beta_i$-Key* | *11* | *$\beta_i = \beta_{i+1}$* |
| *4* | *Do* | *12* | *Else* |
| *5* | *Display Ciphertext* | *13* | *$i = i + 1$* |
| *6* | *While $i > 1$ AND $i == n$* | *14* | *Move to Line 3* |
| *7* | *Else* | *15* | *End* |
| *8* | *If ($\alpha_i$!= $\alpha_{i+1}$)* | | |


Begin
Take plaintext
Perform i-transform with $\alpha_i$-Cipher and $\beta_i$-Key
Is $i > 1$ AND $i == n$?
YES
Display Ciphertext
End
NO
Is $\alpha_i$ != $\alpha_{i+1}$?
NO
Is $\beta_i$ != $\beta_{i+1}$?
NO
YES
$\beta_i = \beta_{i+1}$
YES
$\alpha_i = \alpha_{i+1}$
$\beta_i = \beta_{i+1}$
$i = i + 1$

Where,
**n** is the order number of the multilevel scheme
**i** is the incremental variable
**!=** is the not equal to sign
**=** indicates assignment function
**$\alpha_i$** is the type of Cipher used per **i**-operation
**$\alpha_{i+1}$** is the next Cipher to use after **i**-operation
**$\beta_i$** is the key used per **i**-operation
**$\beta_{i+1}$** is the next key to use after **i**-operation
**AND** is the logical AND-operation

Figure 1: Flowchart Representation of the Generalized Multilevel Scheme

## 4.3 Analyzing the security capability of Multilevel Cryptography

As stated earlier, the security of a multilevel cryptosystem is dependent on the complexity and the structure of its component cipher(s) which can be made more stringent by using more than one type of cryptosystem or the same cipher with different keys. It also depends on the key-length: the length of a given key has much to do with the security of a multilevel structure. It affects the possibility of factoring the key components as well as the possible permutations that can take place in order to realize the plaintext. The order-number of the multilevel cryptosystem, **n**, determines the number of transformations that was performed per given implementation, and helps to keep the implementation tight. The security of a multilevel structure also depends on the complexity and type of the cipher. This determines whether the public has the key of a particular individual or if it is only a selected partner as may be the case for asymmetric and symmetric key cryptosystems respectively.

Key management could also be seen as a serious security implication in a multilevel state. For instance, in an SCSK implementation with symmetric cipher, key revelation could be a great challenge as continuous trials of reverse computation could reveal the ciphertext in clear text. The type of programming language used for the implementation of the multilevel structure also has a great impact on the security of the system.

## 5 Cryptanalysis: Possibility of Multilevel Encryption

In a multilevel state, there still exist possibilities of cryptanalyzing the ciphertext (output). These possibilities could be caused mainly by the factors below:

a. Weakness of the selected cipher(s)
b. Weakness of the programming language used for the system construction.
c. Key management
d. Number of transformations made (order number of the multilevel scheme)
e. Number of cipher(s) used

### 5.1 Weakness of the selected algorithms

In cryptography, most of the often known algorithms have their corresponding weaknesses. These weaknesses have made it variably possible to break the security it ensures and hence keeps the study (cryptography) dynamic. The weakness associated with a particular cipher is different from the one associated to another, and depends on the type of cipher. For instance, if an implementation contains shift-cipher under the modulus of 26; the possible permutations that can be made to realize the security at that level is 26, which is very small to ensuring that the security of information is kept.

### 5.2 Weakness of the Programming Language used for the System Construction

The type of programming language selected for the implementation helps to ensure the total security of the encryption scheme in an application level environment. This is dependent on the security of the construct made with the programming language. Some programming languages are prone to attacks such as: buffer overflow attack, SQL injection attack etc.

These attacks can also be realized if it is used for the implementation of multilevel scheme, so it is advisable to use a programming language that is devoid of attacks for the implementation of multilevel cryptography.

### 5.3 Key Management

Key management is paramount in ensuring the security of multilevel scheme; this has to be built upon trust of the individuals involved on the communication. Some cryptographic ciphersare not public key based and hence are not supposed to be revealed to the public except to those involved in the communication. Thus multilevel cryptographic keys should be kept secret among those that use the implementation.

### 5.4 Number of Transformations Made (Order Number of the Multilevel Scheme)

The order number of a multilevel implementation determines the number of encryption operations that have taken place or that will take place per that particular implementation. This also shows how many reverse computations with the ciphers that will take place before the ciphertext can be realized in clear text. Making this number higher helps to achieve a very high level of security. In fact, one of the major features that helps to make a multilevel scheme different from other methods is the ability to keep this order number high with a single implementation. As you could see from the flowchart figure above (Figure 1), the multilevel scheme could only be satisfied if the i-variable is greater than one. Thus the i-operation can only satisfy this condition of becoming equal to n when the value is two and above. Keeping this n value secret also determines the security of a given implementation.

### 5.5 Number of Cipher(s) Used

The number of ciphers used per given implementation is another factor that influences the security of the scheme. If an implementation contains a single type of cryptosystem, when the weakness of the particular cipher is broken, the entire system is broken; but if it contains more than one type of cipher, breaching of one component cipher does not break the system entirely. So using more than one particular cipher is preferable, especially using an implementation that involves both private and public ciphers. The beauty of involving both private and public ciphers in one implementation cannot be over emphasized as it helps to make a multilevel system more resilient against cryptanalysis attack.

## 6 Future Research

The future direction of this research is to implement this n-cryptographic multilevel algorithm and examine its effectiveness and efficiency against the existing methods.

## 7 Conclusion

This research has shown how two or more encryption schemes can be combined to be more effective. The research proposed and examined the benefits and weaknesses of the blended algorithm for multilevel encryption. The success of information security lies on the inability of adversaries to understand the message if intercepted on a communication network. Several contributions have been made in this regard; formulating cryptographic ciphers that helps to transform the plain information into unintelligible format, as this has not realized perfect information secrecy. As the realization of perfect information secrecy remains a dream, using the proposed multiple cryptographic ciphers to transform given information helps to increase the difficulty of cryptanalyzing encrypted information into its plaintext. The proposed algorithm does not give preference to any particular cipher; it presents an avenue for the possibility of such implementation and also classifies the possible implementation according to types. Multilevel cryptography implements multiple cryptographic ciphers onto a single plain text. The plaintext is taken as shown in the flow diagram and transformed with the predetermined ciphers until the order-number of the implementation is reached. The higher the order number of a given implementation, the more secure the resulting ciphertext will be.

## ACKNOWLEDGMENT

The researchers wish to acknowledge Dr Andrew Fluck of the Faculty of Education, University of Tasmania, Locked Bag 1307, Launceston, TAS 7250, Australia for editing this work.

## REFERENCES

[1]. T. A. Akinwale, F. A. Adekoya, and E. O. Ooju, "Multi-Level Cryptographic Functions for the Functionalities of Open Database System". *Computer Technology and Application 2 (2011), Pp. 730-735*, 2011.

[2]. J.S. Gustavus, "Symmetric and Asymmetric Encryption". *Computing Survey.* Vol. 2 (4), pp. 321, 1979.

[3]. J. N. Ugwu, "Multilevel Offline Cryptography Support System". Undergraduate Project, Federal University of Technology, Minna, Nigeria, 2014.

[4]. W. Judy "Notes from her Math 398 course taught in the Spring of 2002 at UNL". Ericsson AB, ERLANG Secure Socket Layer 5.1.1., 2002.

[5]. L. Harn and H. Lin, "A cryptographic Key Generation scheme for multilevel Data Security". *Computers & Security, 9 (6) 539-546***.** Computer Science Telecommunication program, University of Missouri-Kansas City, Kansas city MO, U.S.A, 1990.

[6]. M. Satti and K. Subhash, "Multilevel Indexed Quasigroup Encryption for Data and Speech". *IEEE Transaction Broadcasting 2009*. Authorized Licence use to: Oklahoma State University, 2009.

[7]. N. S. Sikarwar, "An Integrated Synchronized Protocol for Secure Information Transmission derived from Multilevel Steganography and Dynamic Cryptography". *International Journal of Computer Science and Telecommunication, Vol. 3(4)*, 2012.

[8]. A.M. Richard "Codes The Guide to Secrecy from Ancient to Modern Times, Discrete Mathematics and Its Applications'. Taylor & Francis Group, LLC Chapman & Hall/CRC, an imprint of Taylor & Francis Group, 2005.

[9]. R. K. Gawande, P. S. Kulkani and K. A. Ganar, "Multilevel Image Encryption using Chaotic Mapping and Elliptic Curve Cryptography". *International Conference of engineering Innovation and Technology.* ISBN: 978-93-81693-77-3; Nagpur, 2012.

[10]. S. G. Akl and P. D. Taylor, "Cryptographic solution to a multilevel security problem". Proc. Cryp~o-82, Sanla Barbara, CA, AU~USI 23-25, pp. 237-250, 1982.

[11]. S. Chaitanya, B. Urgaonkar, A. Sivasubramaniam, "Multi-Level Crypto Disk: Secondary Storage with Improved Performance vs Security Trade-offs". *Technical Report CSE-09-006,* 2006.

[12]. T. Hardjono and J. Seberry, “A multilevel Encryption Scheme for Database Security”, Department of Computer Science, University College, The University of South Whales. Australian Defense Force Academy Canberra, A.C.T., 2600, 1989.

[13]. D. G. Usha and R. S. D. Wahida Banu, ‘Secure Multilevel Cryptography Using Graceful Codes’. *International Journal of Information and Electronics Engineering, Vol. 2(5).* 2012.

[14]. O. S. Adebayo, V. O. Waziri (PhD), J.A Ojeniyi, S. A. Bashir, A. Mishra, ‘Information Security on The Communication Network In Nigeria Based On Digital Signature’. *International Journal of Computer Science & Information Security (IJCSIS)’.* Vol. 10 (11), pp. 57-63. ISSN 1947-5500, 2012.