Computer Science and Engineering 2013, 3(2): 29-34
DOI: 10.5923/j.computer.20130302.03

Cipher: A Crypto Model for Improving Confidentiality and Non-Tampering of Data

Adetokunbo A. A. Adenowo[1,*], Basirat A. Adenowo[2], Afeez A. Ajasa[1]

[1]Department of Electronic & Computer Engineering, Lagos State University, Lagos, Nigeria
[2]Department of Computer Sciencet, AdeniranOgunsanya College of Education, Oto-Ijanikin, Lagos, Nigeria

Abstract Vital data and information stored and transmitted on electronic and communication devices are usually subjects of several forms of threat. Ensuring their confidentiality and non-tampering becomes imperative. To curtail such threats, a cryptographic model is proposed and implemented base on a methodologyunderpinned by four key philosophies. The time analysis that indicates the: best, average and worst case analysis was undertaken to determine the effectiveness of the model in expanding attackers' space in attempts to enhance the security of data/information. The analysis reflects a linear proportionality of encryption with respect to size of data. The result reflects an expansion of the search space for the cryptanalyst (i.e. an attacker) to break through the security level achieved.

Keywords Confidentiality, Non-tampering, Cryptographic Model, Encryption, Cryptanalyst, Time Analysis, Security

1. Introduction

Enormous and highly confidential data and information can be found on computer devices and usually transmitted through computer networks. Ensuring data and information confidentiality and protecting from tampering becomes serious issues that should be given considerable attention. Traditionally, Cryptography serves this purpose.This work, therefore, discusses a cryptographic model that can be used to improve the security of data/information.

Cryptography—from the Greek wordsKryptos, "hidden", and graphein, "to write"—isthe study of means of converting information from its normal, comprehensible format, rendering it unreadable to third party.[4] defines cryptograph as the communication in the presence of an adversary andencompasses encryption, authentication, key distribution to mention few.

Historically, cryptography helped to ensure secrecy in important communications, such as those of spies, military and diplomats. In recent decades, the field of cryptography has expanded its remit in two ways. Firstly, it provides mechanisms for more than just keeping secrets: schemes like digital signatures and digital cash, for example. Secondly, cryptography has come to be in widespread use by many civilians who do not have extraordinary needs for secrecy, although typically it is transparently built into the infrastructure for computing and telecommunications, and users might not be aware.

* Corresponding author:
adetokyom@yahoo.com (Adetokunbo A. A. Adenowo)
Published online at http://journal.sapub.org/computer

Cryptanalysis is the opposite of cryptography. It is the study of how to circumvent the use of cryptography; that is, the process of discovering protected information or its key [14],[15]. Cryptography and Cryptanalysis (also known as code-breaking) are sometimes grouped together under the term cryptology. The original information which is protected using cryptography is called the plaintext.

Encryption is the process of converting plaintext into an unreadable form, termed ciphertext, or, occasionally, a cryptogram. Decryption is the reverse process, recovering the plaintext back from the ciphertext. Enciphering and deciphering are alternative terms. A cipher is an algorithm for encryption. The exact operation of ciphers is normally controlled by a key – some secret piece of information that customises how the ciphertext is produced.

Encryption is a subsystem that transforms the plain data into an unintelligible form while Decryption subsystem transforms the inverse when required. Both subsystems require a key for successful operation and the transformation process may be transposition of symbols in the plain text or substitution of symbols with some cipher characters.

The use of cryptography techniques often employs both permutations and pseudorandom numbers and can be cracked by a cryptanalyst or eavesdropper based on the following:

- Predictivity of pseudorandom number sequences employed in the substitution ciphering technique.
- Predictivity of permutation patterns employed in transposition ciphering technique.
- Generation of a table of all possible decrypted data of a cryptogram if the algorithm is known and if the encryption key repertoire is small.

Due to the above problem, this work aims at finding a

solution or at least minimizes the problems. To achieve this aim, a conceptual model is proposed and implemented through the enlargement of potential cryptanalyst's search space without over tasking the user.

2. Related Work

Cryptographic schemes have been employed in several security related works, ranging fromvisual to non-visualbased cryptographic schemes, in attempts to secure data, information and/or signals.[7] considers the authentication of remote credit card users. The work aimsunauthorised access to credit card by securely authenticating the location of mobile users using non-visual cryptographic techniques. Thesystematic approach introduced generates encrypted data to user's mobile number along with decrypting key as SMS only when the location of the credit card matches that of the user's mobile number. Despite the approach, the SMS appears prone to interception even when the locations matcheach other, thereby givingroom to manipulation of transmitted information.

[11] investigatesthe integrity protection of navigation signals. The paper proposes practical solution that is based on short-term information hidingwhich attempts to prevent access by an attacker to navigated signals. Operationally, when a weak spread-spectrum broadcast signal is initiated from a Global Positioning System (GPS), the signal is temporarily hidden in background noise while the receiver system buffers the entire radio band in its RAM. The required decryption key is only published after a quantum amount of time when both a signal-synthesis and a selective-delay attack can easily be identified. Despite this effort,[11] acknowledged that the approach—based on temporary key hiding—is still open to attack by relaying attacks on the transmitted signals.

Aside the above non-visual cryptographic techniques,[6] propose a two-fold security measure towards securing an iris template. This involves the combination of biometric and visual cryptography, necessitated by the vulnerability of Biometric systems to attacks thus limiting or reducing their security. To prevent plaintext storage of biometric templates and to provide fool-proof methodologies to secure them, they evolve the combination of biometric and visual cryptography.

Also,[1] employs visual cryptographic technique base on a biometric code that is watermarked in a document with a secret key. The resultingdocument is a biometric watermarked document that authenticates the real owner, which can be de-watermarked with the same secret key in order to authenticate it.As claimed by the latter, experimental results indicated that the approach was effective in authenticating thegenuine documents. Several other research efforts have highlighted visual cryptography schemes toward improving security of information and these can be found in the literature (see[5],[9],[12], and[13]).

3. Methodology

After considering a number of factors including a number of International Data Encryption Standards (see[14]), the design philosophy of the conceptual cryptographic model proposed consists of the following:

- Provision of a high level of information security against unauthoriseddisclosure, that is, ensuring the confidentiality of information.
- A protection based on the secrecy of the encryption key and not the secrecy of the algorithm.
- An encryption algorithm adaptable to use in diverse applications (that is, current work not restricted to a specific application context like previous works).
- Easy user interface.

The algorithm for the proposed cipher model, though not "tour de force", is envisaged to provide an enhanced level of security. The protection mechanism combines: transposition and substitution methods, through dynamic permutation, non-linear pseudorandom number sequence and non-secrecy of the algorithm. Although, this work employs secret key, similar to previous works mentioned in section 2.0 above, current work emphases the non-secrecy of the algorithm implemented and combination of protection mechanisms' to evolve the secret key. Also, this work contrast to the above cited instances in that it is not context-based (e.g. Credit Card, GPS, etc.), thus, provides wider application in diverse areas.

3.1. Dynamic Permutation

Transposition ciphers on their own are easy to crack but have been found useful if combined with substitution ciphers. Unlike many contemporary transposition systems where the sizes of the permutation blocks are fixed, the approach employed varies the size of each block with each data element constituting the record to be encrypted. The permutation patterns are as shown in figure 1 below.

Permutation Patterns	
Order of Plain Characters	Encrypted Form
1	1
1 – 2	2 – 1
1 -2 – 3	2 – 3 – 1
1 – 2 – 3 – 4	2 – 4 – 1 – 3
1 – 2 – 3 – 4 – 5	3 – 2 – 5 – 1 – 4
1 – 2 – 3 – 4 – 5 – 6	4 – 2 – 6 – 1 – 5 – 3 etc.

Figure 1. Permutation Patterns

3.2. Non-Linear Pseudorandom Random Number Sequence

The substitution system for the proposed model is basedon two-stage pseudo-random number (PRN) generators: a seed-stage and a key-stage (see[14], pp. 44-45 for types of random number generators). The seed-stage uses "multiplicative congruential" PRN generator, modelled as indicated thus:

$$S_{i+1} = QS_i \bmod T, \quad i = 0,1,2\ldots\ldots\ldots 50 \quad \text{eqn. (1)}$$

where S_{i+1}--is the new uniform deviate,

S_i--is the previous uniform deviate,

Q--is a constant, and

$S_{i=0}$--is the initial seed and is derived by summing the ASCII equivalents of the encryption key characters.

With the above, we generate 50 seeds that we store in a hash table. The best results for the multiplicative congruential method on a binary cipher machine can be achieved when S = 8T + 3,T(an integer) = 2b where b > 2 and is usually selected to be the word length of the machine and the period is T/4 (See also[2],[3],[8] and[9]).

The Key-stage is based on "mixed congruential" PRN generator with the formula:

$$r_{i+1} = (Br_i + C) \bmod T \quad \text{..... Eqn. (2)}$$

where r = f(H, n, k),

H =seed hash table entries,

n =the record position in a sequential file orthe record key for a direct access file, and

k_1 =the first subkey from the set (k_1, k_2, ...k_{12}).

r_0 serves as the starting seed for each record to be encrypted. Non-linearity is introduced into the key sequence actually used for substitution by alternating between discarding k_i generated PRNs and using the next one, where k_i's are the encryption subkeys. These subkeys are the least significant digits of the ASCII equivalents in decimal of the encryption key characters. Since the resultant subkeys in most cases will have different values, the intervals between successively used PRNs will vary and hence make cryptanalysis based on predictivity of the PRN sequence more difficult.Note that[10] has shown that the period of this generator will be T if and only if,C is odd, andB mod 4 = 1.

3.3. Non-Secrecy of Ciphering Algorithms

This requirement is due to the impossibility of ensuring absolute non-disclosure of protected programs in shared environments. The suggested method aims at making this non-issue by making the protection dependent on the secrecy of the encryption key and less on the secrecy of the cipher algorithm. Thus, an attacker will only crack this system if the following can be accurately guessed:

- The varied permutation patterns
- The initial seed
- The number values and order of the subkeys.

4. Proposed Model

The cipher model, an experimental implementation of the cipher methodology, is targeted as a library of algorithms that provides diverse applications with a file ciphering subsystem. Storage and retrieval of information, using this model, is done through the cipher model. See figure 2 below which represents the structure of the proposed cipher model. The model encrypts at the point of storage and decrypt at the point of retrieval. The function of the components depicted in the Cipher structure is given below.

a. User Interface – the users are required to process cryptographic files via the user interface of the model. Such process may be storage or retrieval of records. The user interface consists of a data space, file description and a set of commands.

- Data space – the space or variables for transmitting or receiving data constituting each record between the user program and the proposed model, Cipher.
- File Description – a description of each crypto-file to be processed. It consists of the file name, file number, file type, file mode, record length, record format, and cipher key.
- Command construct – the user program exploits the facilities provided by the model (i.e. Cipher) with the aid of some command constructs that invoke the appropriate modules to carry out the desired operation. These constructs include:

i. Cipher Initiation – prepares the environment necessary for ciphering operations.

ii. Crypto-file Specification – after describing the file and records to be ciphered, this command instructs Cipher to validate and note them for subsequent references. It calls the crypto-file specification module into action..

iii. Encipher a Record – instructs Cipher to read a scrambled record from some storage medium and decipher it.

iv. File Closure – instructs Cipher to close a processed file and moves its details from the cipher tables.

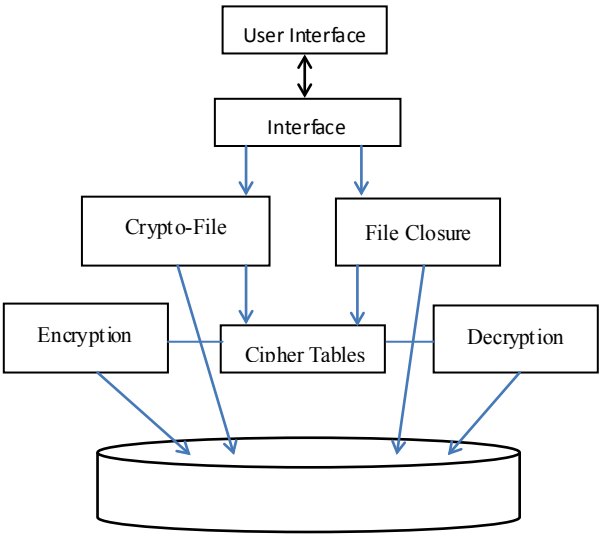

Figure 2. Cipher Model

b. Interface Module– This module links the user program with the cipher system. It validates and interprets the commands issued by the user programs and calls the appropriate routine to carry out the operation. The input is a user command and output is the cipher tables, and the pseudo-code or algorithm utilised is given thus:

1. Start
2. Test for validity of user command and exit if invalid.
3. Save variable with names common to the user program and cipher.
4. If user command is to initiate cryptosystem then define the required cipher tables else invoke the appropriate routing

to carry out the command.

5. Restore to user program.

6. Exit to user program.

c. Cipher Tables– These contain data employed for ciphering activities; they include:

- File description table
- Record format table
- Encryption subkeys table; and
- Hash table for PRN seeds.

d. Crypto-File Specification– This module creates the relevant Cipher table entries for each user file to be ciphered. The input is made up of file description, record format, encryption key and cipher tables. The output generated is the cipher tables. Algorithm used is as follows:

1. Entry

2. Validate the file and record descriptions specified by the user and enter the corresponding cipher table.

3. Request for the file's cipher key.

4. Convert each key character into its numerical ASCII equivalent in decimal.

5. Sum the results in step 4 to give the initial seed for the PRN seed-stage.

6. Create a set of subkeys: k_1, k_2, ……, k_{12}, by extracting the I.S.D. of the numerical equivalents of the key characters obtained in step 4. Enter these into the subkey table.

7. Create the seed sequence based on a multiplicative congruential PRN generator (see eqn. 1 above) and store in the seed table.

8. Open the desired file.

9. Exit.

e. Encryption Module– The module scrambles the user records using a combine approach of transposition and substitution methods as earlier mentioned. The input into the module are vector of user supplied data elements, file name or number, records' key if a direct access file, and cipher tables. The output is Cryptogram written to the specified file. The algorithm adopted is as follows:

1. Entry

2. Compute the seed for the key-stage PRN generator based on the method described in section 3.2.

3. Perform step 4 through 7 for each data element constituting record.

4. Break the element into its component characters.

5. Permute these characters based on the permutation pattern described in section 3.1.

6. Perform substitution for each character based on the method described in section 3.2.

7. Add the data element to the record buffer.

8. Write the record to the file.

9. Exit

f. Decryption Module–It de-scrambles any information earlier scrambled by the encryption module provided the appropriate encryption key is given. The input into this module are file name or number, record's key if a direct access file, and Cipher tables. The module generates an output of plain data elements. The algorithm for the module is:

1. Entry

2. Compute the seed for key-stage PRN generator based on the method described in section 3.2.

3. Read a record.

4. Break a record into its component data element using the record format specification.

5. For each encrypted data element perform step 6 through 9.

6. Break the data element into its component characters.

7. De-permute these characters.

8. Perform de-substitution of the characters to realise the original plain characters.

9. Combine the resultant characters to yield the original plain data.

10. Exit.

g. File Closure Module– This module closes all used files and clear used memory spaces to avoid inter-file interference, and sensitive residue. The inputs into the module are File number and Cipher tables. No output is generated. The algorithm implemented is:

1. Start

2. If end of all crypto-section, then clear all cipher tables from memory else clear part of cipher tables which were used for the particular file.

3. Close the files or file.

4. Exit.

5. Result and Discussion

The results achieved are presented in this section as well as the performance and analysis of Cipher. Though a variety of factors can be employed in evaluating any software, the performance criteria for Cipher are:

- The file ciphering capability
- Degree of security provided; and
- Execution time.

5.1. File Ciphering Capability

This aspect is handled by two algorithms designed to test the ability of Cipher to handle different file organisations, namely: sequential and random access files. The algorithms incorporate a facility for viewing the content of the crypto-files in order to ascertain their ciphering capability.

5.2. Degree of Security

This cipher methodology herein described employs dynamicpermutation and non-linear pseudorandom number sequence as means to avoiding weaknesses like predictivity of fixed block permutation patterns and continuous pseudorandom number streams. Allowing keys of variable lengths (8-12 characters inclusive) and encrypting each record with a relatively unique initial seed has further enlarged the search space for the cryptanalyst. This need is a function of:

- Some hash seed
- The most significant subkey; and

● The record key for random access files or the position of a record in a sequential file.

Thus, for none-easily compromised keys, cracking cipher based on its library of algorithms would theoretically require guessing the following:

i. The initial seed used in enciphering each record.

ii. The number, values and order of the encipher sub key.

iii. The algorithm and record format if not known.

However, the ultimate test for the degree of security is an assault on the system by skilled cryptanalyst.

5.3. Execution Time

The major determinant of the rate of encryption and de-encryption are the number of characters per record and the average values of the encryption subkey. The subkeys vary between 0 and 9 inclusive and determine how many pseudorandom numbers (PRN) are discarded for each encrypted characters in order to achieve non-linearity. An attempt has been made at measuring the encryption time expendable for minimal or best, average and worst time efficiencies. Table 1 shows the measurement made while figure 3 belowrepresents the graph plotted using the values in the table for the three cases.

Table 1. Execution Time Measurement

Characters per Record	40	60	80	100	120
Best case (secs.)	2.3	3.0	3.6	4.5	5.3
Average case (secs.)	2.9	3.9	4.8	6.3	7.3
Worst case (secs.)	3.5	4.9	6.5	7.8	9.3

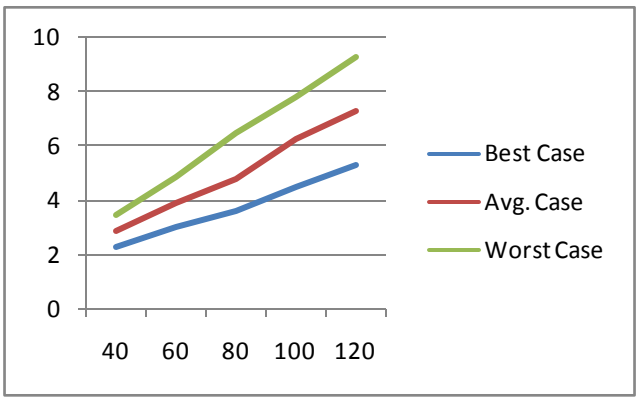

Figure 3. Execution Time Measurement Graph

The graph shows that the encryption time for each case is linearly proportional to the size of the record. This can be expressed mathematically as: $T_b(n) = O(n)$; $T_a(n) = O(n)$; and $T_w(n) = O(n)$ — where T_b, T_a and T_w denotes the best, average and worst requirement, n denotes the record size and O denotes the order of magnitude.

However, the best time case negates a major objective of this design since it implies no PRN are discarded. That is, a linear sequence of PRNs is employed hence exposing the cipher to attack by predictivity of pseudorandom number sequences. This degenerates case can be avoided if all the key characters are not chosen from the following set:

SET: (2: f p z d n x) – list of characters which generates subkeys with zero. Note that the measurement for decryption gave similar results.

6. Conclusions

This work, however, demonstrated that a cryptographic model can be useful for securing confidential/vital data and/or information in transit or storage against unauthorised disclosure (or tampering). It enhances a security system such that if the conventional security strategies are penetrated, some cryptanalytic efforts must be expanded before accessed information can be comprehended.

The required cryptanalytic effort can be increased through various methods including dynamic permutation and non-linear pseudorandom number sequence applied in the above model. However, effective and efficient security requires an integration of different security strategies commensurate with the computing environment.

REFERENCES

[1] Anitha, V. &Velusamy, R.L., 2012, Authentication of digital documents using secret key biometric watermarking, InternationalJournal of Communication Network Security, 1(4), pp.5-11.

[2] Downham, D.Y. & Roberts, F.D.K., 1967, Multiplicative congruential pseudo-random number generators, The Computer Journal, 10(1), pp.74-77.

[3] Fishman, G.S., 1990, Multiplicative congruential random number generators with modulus 2^{β}: an exhaustive analysis for $\beta = 32$ and a partial analysis for $\beta = 48$, Mathematics of Computation, 54(189), pp. 331-344.

[4] Goldwasser, S. &Bellare, M., 2008, Lectures notes on cryptography, Cambridge: Massachusetts.

[5] Guo, T., Liu, F., Wu, C. &Hou, Y., 2012, Using variance to analyze visual cryptography schemes, International Association for Cryptologic Research (IACR) ePrint Archive, 2012: 315.

[6] Hajare, N., Borage, A., Kamble, N.&Shinde, S., 2013, Biometric template security using visual cryptography, International Journal of Engineering Research and Applications, 3(2), pp. 1320-1323.

[7] Hemamalini, S, Dillirani,S., Girija,G.G. &AlphinEzhil Manuel, M.L., 2012,Credit card forgery identification system with location based tracking using mobiles with GPS, International Journal of Communication Network and Security, 1(3), pp. 58-63.

[8] Hull, T.E.&Dobel, A.R., 1962, Random number generators, SIAM Review, 4 (3), pp.230-254.

[9] Hull, T.E. &Dobel, A.R., 1964, Mixedcongruential random number generators for binary machines, Journal of Association of Computer Machine (ACM), Vol. 11, p.31.

[10] Kandari, S., Maiti, A. &Dhara, B.C., 2011, Visual

cryptography scheme for color image using random number, International Journal of computer Science, 8 (3), No.1, pp. 543-549.

[11] Knuth, C., 1969, Cryptography and information theory.

[12] Kuhn, M.G., 2005,an asymmetric security mechanism for navigation signals, In J. Fridrich (Ed.): Information Hiding, Lecture Notes in Computer Science 3200, pp.239-252. Berlin Heidelberg: Springer-Verlag.

[13] Revenkar, P.S., Anjum, A. &Gandhare, W.Z., 2010a, Survey of visual cryptography schemes, International Journal of Security and Its Applications, 4(2), pp. 49-56.

[14] Revenkar, P.S., Anjum, A. &Gandhare, W.Z., 2010b, Secure iris authentication using visual cryptography, International Journal of Computer Science and Information Security, 7(3), pp.217-221.

[15] Stallings, W., 2013a, Network security essentials: application and standards, 5th Edition. New Jersey: Prentice Hall.

[16] Stallings, W., 2013b, Cryptography and network security: principles and practice, 6th Edition. New York: Prentice Hall.