(https://www.psychosocial.com)

International Journal of Psychosocial Rehabilitation

ISSN:1475-7192

Login/Register (/register-login)

International Journal of Psychosocial Rehabilitation

ISSN : 1475-7192

Chief Editor Name : Dr. A.J. Anderson

Publisher Name : Hampstead Psychological Associates

Descriptions :

A WEB BASED PEER REVIEWED PUBLICATION FOR MENTAL HEALTH PRACTITIONERS, CONSUMERS & APPLIED RESEARCHERS

This private NON-PROFIT professional publication and associated web-based, information archive service is dedicated to the enhancement of practice, program development, program evaluation and innovations in mental health and substance abuse treatment programs worldwide. Its goal is to provide a public forum for practitioners, consumers and researchers to address the multiple service needs of patients and families and help determine what works, for whom under a variety of circumstances.

Submit Online (/submit-online)

For authors

Scope (https://www.psychosocial.com/scope/)

Track Your Paper (https://www.psychosocial.com/track-your-paper/)

Submit Online (https://www.psychosocial.com/submit-online/)

Editorial Overview (https://www.psychosocial.com/editorial-overview/)

Instructions for Authors (https://www.psychosocial.com/instructions-for-authors/)

Privacy & Cookie Policy (https://www.psychosocial.com/privacy-cookie-policy/)

Terms & Conditions (https://www.psychosocial.com/terms-conditions-of-use/)

(https://www.scimagojr.com/journalsearch.php?

q=17700156008&tip=sid&exact=no)

(https://www.scopus.com/sourceid/17700156008?dgcid=sc_widget_citescore)

0.19 2018
CiteScore

16th percentile

Powered by (https://www.scopus.com/sourceid/17700156008?dgcid=sc_widget_citescore)

(https://www.scopus.com/sourceid/17700156008?dgcid=sc_widget_citescore)

EBSCO

Quick Links

About Publisher (https://www.psychosocial.com/about-publisher/)

Copy Rights (https://www.psychosocial.com/text-book/)

Contact Us

editor@psychosocial.com (mailto:info@jof-cis.com)

Hampstead Psychological Associates,
Suite B19, 110 Gloucester Road,
London, NW1 8JA.
United Kingdom

(https://www.psychosocial.com)

International Journal of Psychosocial Rehabilitation

ISSN:1475-7192

Psychology

Applied psychology
Biological psychology
Clinical psychology
Developmental psychology
Experimental psychology
Cognitive neuroscience
Educational psychology
Mathematical psychology
Social psychology
Psychoanalysis

Psychiatry and Mental Health

Mental health
mental illness
Psychological disorders
Attention Deficit Hyperactivity Disorder (ADHD)
Bipolar Disorders
Behavioral disorders
Sleep Disorder
Panic Disorder
Serious Emotional Disturbance (SED)
Anxiety
Depression
Autism

Nursing

Evidence-Based Nursing
Clinical nursing
Care of the chronically ill
Community care
Care of older people
Pediatrics nursing
Emergency nursing Neonatal care
Trauma nursing
Wound, ostomy, and continence nursing

Gastroenterology nursing
Health care management
Infant and young children nursing
Addictions nursing

Biological and Medical Sciences

Biology
Life Science
Anatomy
Botany
Cytology
Genetics
Microbiology
Physiology
Zoology

Ecology
Environmental Sciences

Educational Research

Teaching and Learning
Learning Theories and Teaching Methodologies
Educational Psychology
Philosophy of Education
Sociology of Education
Special Education
Literacy
Primary
Secondary and Higher Education
Educational Management
Leadership and Management
Educational Research
Curriculum and Instruction
Educational Change
Teacher Education
Pre-service and In-service Teacher Education

Management Sciences and Economics

Human Resource Management
Business Management
Financial Management
Organizational Behaviour
Strategic Management
Public Sector Management
Research & Development
Organizational Management
International Management
Project Management

Project Management
Industrial Management
Marketing Management
Management Theories and Practices

Social Sciences, Arts and Humanities

Anthropology
Cultural studies
Educational Research
Ethnicity and Racism Studies
Gender Studies
Geography
Interdisciplinary Social Sciences
Labour Studies
Language and Literature
Religious Studies
Psychology
Social Work
Sociology
History
Philosophy
Library Studies
Museum Studies and other areas related to social sciences
arts and humanities

Sports Sciences

Sports Performance
Physiology and Nutrition
Physical Activity, Health and Exercise

Others

Anthropology
Applied Linguistics
Applied Physics
Architecture
Artificial Intelligence
Astronomy
Biological Sciences
Botany
Chemistry
Communication studies
Computer Sciences
Computing technology
Cultural studies
Design
Earth Sciences
Ecology
Education

Electronics
Energy
Engineering Sciences
Environmental Sciences
Ethics
Ethnicity and Racism Studies
Fisheries
Forestry
Gender Studies
Geography
Health Sciences
History

Interdisciplinary Social Sciences
Labour studies
Languages and Linguistics
Law
Library Studies
Life sciences
Literature
Logic
Marine Sciences
Materials Engineering
Mathematics
Media Studies
Medical Sciences
Museum Studies
Music
Nanotechnology
Nuclear Physics
Optics
Philosophy
Physics
Political Science
Psychology
Social Work
Sociology
Space Sciences
Statistics
Transportation
Visual and Performing Arts
Zoology and all other subject areas

For authors

Scope (https://www.psychosocial.com/scope/)

Track Your Paper (https://www.psychosocial.com/track-your-paper/)

Submit Online (https://www.psychosocial.com/submit-online/)

Editorial Overview (https://www.psychosocial.com/editorial-overview/)

Instructions for Authors (https://www.psychosocial.com/instructions-for-authors/)

Privacy & Cookie Policy (https://www.psychosocial.com/privacy-cookie-policy/)

Terms & Conditions (https://www.psychosocial.com/terms-conditions-of-use/)

(https://www.scimagojr.com/journalsearch.php?q=17700156008&tip=sid&exact=no)

(https://www.scopus.com/sourceid/17700156008?dgcid=sc_widget_citescore)

0.19 2018 CiteScore

16th percentile

Powered by Scopus (https://www.scopus.com/sourceid/17700156008?dgcid=sc_widget_citescore)

(https://www.scopus.com/sourceid/17700156008?dgcid=sc_widget_citescore)

EBSCO

Quick Links

About Publisher (https://www.psychosocial.com/about-publisher/)

Copy Rights (https://www.psychosocial.com/text-book/)

Contact Us

editor@psychosocial.com (mailto:info@jof-cis.com)

Hampstead Psychological Associates,
Suite B19, 110 Gloucester Road,

London, NW1 8JA.
United Kingdom

INTERNATIONAL JOURNAL OF PSYCHOSOCIAL REHABILITATION

editor@psychosocial.com

Mar, 19, 2020

Dear, Marwah Kamil Hussein[1] , Kasim Al-Salim[2], Asaad Alhijaj[3]

1University of Basra, College of Computer Science and Information Technology, Computer Information Systems Dept..
lava85k@gmail.com
2 University of Basra, College of Computer Science and Information Technology, Computer Dep.
Kasim.alsalim@gmail.com
3 University of Basra, College of Computer Science and Information Technology, Computer Information Systems Dept.
1,2,3Basra, Iraq , Zenhjaj@yahoo.com

We would like to inform you that your manuscript has been accepted for publication in **International Journal of Psychosocial Rehabilitation (ISSN 1475-7192).**

Manuscript Title: " Hybrid Method For Encoding Of Genetic And RC4 Algorithms "

Thanks for submission of your work with us.

Regards,

Professor Dr. Jacob lewis.

Associate Editor
International Journal of Psychosocial Rehabilitation (ISSN 1475-7192).

Hybrid Method For Encoding Of Genetic And RC4 Algorithms

Marwah Kamil Hussein[1], Kasim Al-Salim[2], Asaad Alhijaj[3]
[1]*University of Basra, College of Computer Science and Information Technology, Computer Information .Systems Dept.*
lava85k@gmail.com
[2]*University of Basra, College of Computer Science and Information Technology, Computer Dep.*
Kasim.alsalim@gmail.com
[3]*University of Basra, College of Computer Science and Information Technology, Computer Information Systems Dept.*
[1,2,3]*Basra, Iraq*
Zenhjaj@yahoo.com

Abstract

In this paper, the proposed new method used is to generate the encryption key used in the RC4 algorithm by using the genetic algorithm by randomly generating it using the Rand function, and then subjecting it to the randomized conditions approved. If a match is used for coding, otherwise the genetic algorithm will be used to generate the random genetic key, which is along the length of the text to be encrypted.The proposed method used a new structure to hide the encrypted key within the transferred text, in addition to the integrity of the transferred key (integrity) was confirmed by using a simple flux function.

Keywords: *Coding, RC4, Genetic Algorithms, Voice, Hash Algorithm.*

1. Introduction

Information security at the world level is an obsession and concern for those in charge of managing various information systems, especially in light of the growing information crime operations that imposed the need for concerted efforts by all countries and governmental and private institutions worldwide, including individuals, to eliminate all violations of information security In particular, in light of the development of technology and the spread of risks involved in its various uses and applications [1].

The term information security is defined in its broad and comprehensive concept as a set of procedures that enables the owner of the information to keep his personal information, data and financial and bank accounts under his full and direct control, and not to allow any unauthorized person to access it with a view to circulating it either in good faith or in bad faith or with the aim of blackmail and tampering It out. Security dysfunctions in information security systems usually occur when the systems are compromised through, for example, hackers, viruses, or any other type of malicious program. Information security professionals strive to ensure the integrity of the various information systems by achieving three basic requirements, which are confidentiality of information, integrity of information, and availability of information [2].

- The fulfillment of the first requirement related to confidentiality of information requires that information be secured in a way that only authorized persons can access it (others with authority or authorized).
- As for the second requirement of confidentiality of information, it seeks to ensure the integrity of the sources of information, so that it cannot be changed or updated only by authorized persons only.
- The third requirement to ensure information security is the possibility and ease of providing information when it is needed. There are also a number of elements that weaken the security systems of different networks and steal information, among which are, for example, password leaks, electronic eavesdropping, hacking, viruses, lures, and identity theft [3][4].

From this standpoint, we know the extreme importance that necessitated the attention of states, governmental and private institutions and individuals, and in light of the development of technology and the spread of risks that have become a problem for societies, technology despite its great services to the human being in the modern era, but it is like any other invention that has many advantages and has serious drawbacks if it does not identify It has to work to avoid it, and in the context of our research we discussed methods and tools to protect the information security of the average user in using the RC4 encryption algorithm [5].

RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code"[6] . The RC4 name is trademark, so RC4 is often referred to as ARCFOUR or ARC4 (this means the alleged RC4) [12] to avoid trademark problems [7].

Noting these advantages, the GA algorithm was used in this research to generate the encryption key used in the RC4 algorithm. After reviewing some previous research that dealt with the uses of GA with coding and decoding, for example:

Where researcher [8] has used the genetic algorithm to find the best key to use for encoding texts in a compensatory coding method (Substitution cipher). As for the researcher [9], GA was used to find the length of the secret key that will be used in the analysis of the Permutation cipher. In addition, the search used [10] GA to break the cipher transposition encoded text, and finally researchers [11] introduced three methods of guesswork intuition to reach optimization: (used in the simulation (annealing, genetic algorithm), which was used in the used Transposition cipher [12].

In this research, the genetic algorithm was utilized by proposing a new method for generating the random key used in the RC4 algorithm.

2. Stream Cipher Of Rc4 Algorithm

- Stream cipher operate on a stream of data, one byte at a time.
- Typically stream ciphers perform an Exclusive OR(XOR) operation on a stream of plaintext bytes with the key stream from a pseudo random number generator (PRGA).
- Decryption is achieved by the same byte wise XOR operation on the cipher text.
- Fast and easy to implement in hardware.
- PRGA guidelines:-
    - The key stream must have a large period making the repetition of the a sequence for a part.
    - The key stream generated should possess as much properties as a true random number generator.
    - The input master key (K) must be as a large as possible. [13][14].

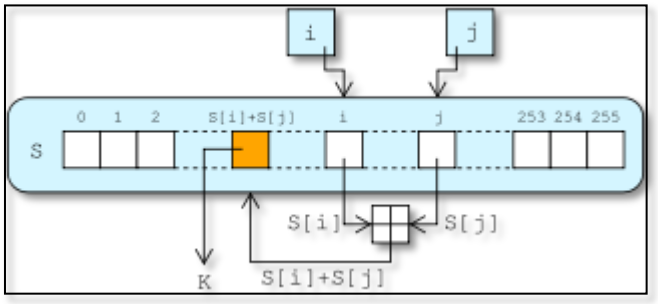


Figure 1. PRGA flowchart.

3. Secure Hash Algorithm (SHA)

Is one of the Hash algorithms that find a constant string of any text or file, there are several types, including: -

SHA1: This algorithm produces a 160 bit (20 byte) key.

SHA512: This algorithm produces a 512 bit (64 byte) key of any message or file of any length and a number of other SHA types as we see it in Figure 4 below and the property of each type. We'll explain in detail how SHA512 works [15][16].

3.1 Part (1):

We know that SHA512 receives any length of data and finds it has a 512 bit HASH length in the Fig. 2. It divides the message into a block each one has a size of 1024 bit and another 128 bit in the last block it is reserved for the length of the real data i.e. this algorithm can find HASH for data with a maximum length of its length 2 ^ 128 and the bits that remain blank between the last 128 bit and the actual data of the message after converting it to binary, we have padding, meaning we enter one number and a number of zeros follow it until we fill in the empty bits. And the last block accepts only 896 bits because as we said the last 128 bits in the last block are reserved for the length of the real message in binary system format where iv = H0 represents the eight registers (A, B, C, D, E, F, G, H) each one of its size 64 bit total is 512 bit which will eventually represent the message's Hash. These are initial values stored within Registers. See Fig. 2 [17].

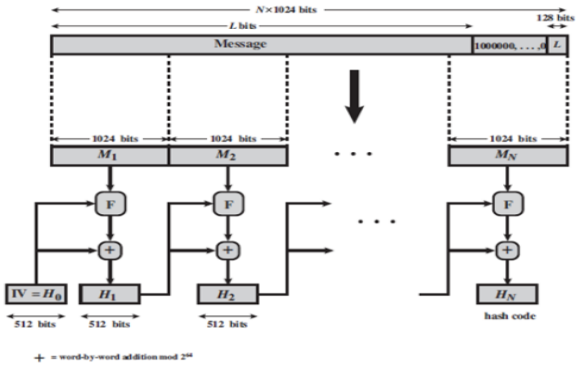


Figure 2.Message digest generation using (SHA-512).

3.2 Part (2):

Which represents Part 2 in the Fig. 2 is the letter (F) in Part No. 1, where it repeats its same operations with each block so we will explain on one Block and the rest of the same thing. Fig.3 represents the operations that will be performed on each block of the real message to produce a key whose length is 512 bits stored in (A, B, C, D, E, F, G, H) and is considered as an entry for operations on the next Block if the data is more than Block As shown in Fig. 3, or the final result is considered if the data is a single block. And that each (F) is divided into 80 Round, each one carrying out the operations inside him once (Part 4 in Fig. 5 represents the operations that will take place within each Round) . In the Fig. 3, each round of 80 is entered with a value of a certain K between (K0-K79), which are fixed values consisting of 64 bits taken from the following table [17].

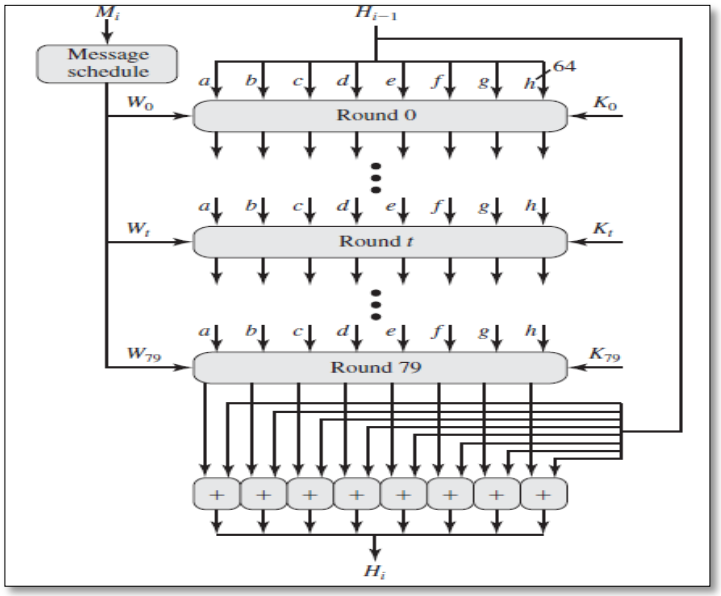


Figure 3. SHA-512 processing of a Single 1024- bit block.

3.3 Part (3):

We also note that in the Fig. 4, each Round enters a value from Block data of 64 bit length and that the length of one Block is 1024 bit, so it divides (1024) into 16 Block, each one of which is 64 bit size represented (W0-W15) and enters the first 16 Round and the rest of Round takes Wt according to the following formula [18].

$W_t = \sigma_1^{512}(W_{t-2}) + W_{t-7} + \sigma_0^{512}(W_{t-15}) + W_{t-16}$

where

$\sigma_0^{512}(x) = ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x)$

$\sigma_1^{512}(x) = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^6(x)$

$ROTR^n(x)$ = circular right shift (rotation) of the 64-bit argument x by n bits

$SHR^n(x)$ = left shift of the 64-bit argument x by n bits with padding by zeros on the right.

+ = addition modulo 2^{64}

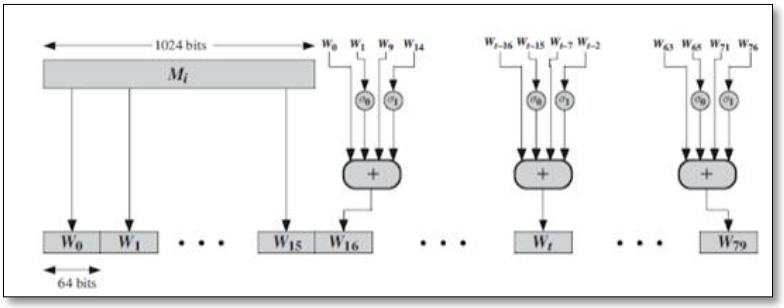


Fig. 4. Creation of 80-word input Sequence for SHA-512 processing of single block.

3.4 Part (4):

Part No. 4 in Fig. 5 represents the operations that will take place within each Round in order to not update them on the Registers values that will consider the updated values as the next Round entry and in the last Round is the Hash of the message if the message is from one block and otherwise it is considered an entry for Registers data in the next Block W_t Block: represents 64 bit of Block data previously explained in preparation for each Round [18]. K_t: These are 64-bit constant values taken from the table previously explained

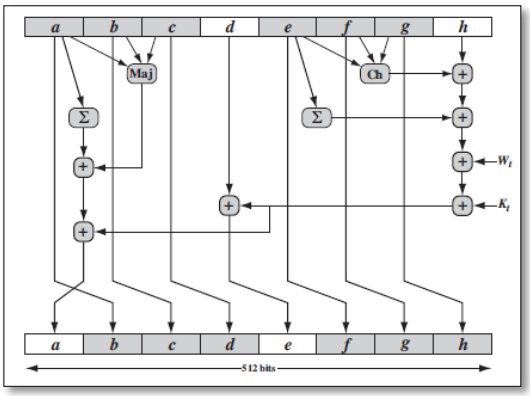


Fig. 5. Elementary sha-512 operation (single round).

$$T_2 = (\sum_0^{512} a) + Maj(a,b,c)$$

$h = g$, $g = f$, $f = e$, $e = d + T_1$, $d = c$, $c = b$, $b = a$, $a = T_1 + T_2$

where

t = *step number*, $0 \leq t \leq 79$

$$Ch(e,f,g) = (e \text{ AND } f) \oplus (\text{NOT } e \text{ AND } g)$$

The conditional function: If e then f else g

$$Maj(a,b,c) = (a \text{ AND } b) \oplus (a \text{ AND } c) \oplus (b \text{ AND } c)$$

The function is true only of the majority (two or three) of the arguments are true

$$(\sum_0^{512} a) = ROTR^{28}(a) \oplus ROTR^{34}(a) \oplus ROTR^{39}(a)$$

$$(\sum_1^{512} a) = ROTR^{14}(e) \oplus ROTR^{18}(e) \oplus ROTR^{41}(e)$$

$ROTR^n(x)$ = circular right shift (rotation) of the 64-bit argument x by n bits

W_t = a 64-bit word derived from the current 512-bit input block

K_t = a 64-bit additive constant

4. General steps of the genetic algorithm:

- Create a primary generation
- Find the function of the objective, the extent of fitness, and the potential contribution to the primary generation
- Sections
- Parent test (Selection).
- Interventional intervention (Crossover)
- Change within one syllable (Mutation)
- Standard for stopping the genetic algorithm [19][20]

5. Research Objective

To obtain more confidentiality, faster implementation and less cost, an algorithm was proposed. Hybrids take advantage of the genetic characteristics to make a key and check its randomness by using approved methods. Instead of regenerating the key at the receiving end, a new method has been used to hide the key. Inside the encoded text before sending, the integrity of the received key has been confirmed by using the SHA camouflage function.

6. Suggested Way to Configure The Key:

Genetic algorithm has been relied upon to avoid behaviors caused by the traditional method. In Initially, a random generation of key is generated using the rand function in Matlab, noting that the length of the key must be the length of the text to be encoded, and then the tribe is measured from the randomness. As per the approved conditions [5], if the conditions are fulfilled, the individual is random and will be used for coding. The whole primary generation does not fulfill the conditions the genetic algorithm is used.

7. Structure of The Proposed Method:

The basis for successful encryption is the approved algorithm and key confidentiality. The following algorithm has been adopted:

- *Algorithm (1)*
  1. Getting Started
  2. Enter the express text to be encrypted
  3. Convert the express text to the binary code using the ASCII code. 4. Calculate the number of bits in which the text is made after converting it to the binary system. 5. The code is shown in the code with the code.
  4. Random Key Test According to Algorithm (2)
  5. In the event that it does not fulfill the conditions of the algorithm (2), the genetic algorithm (3) is used.
  6. If the conditions are met, the key is used to encode the express text using the RC4 encoding method.
  7. SHA Flux Calculation for the key and result set at end of text after encoding
  8. Hide the key within ciphertext according to algorithm (4(
  9. Calculate the number of characters of the original text and place it at the end of the text
  10. Send the message
  11. End.
- *Algorithm (2).*

The approved conditions were used to randomize the test [5] as follows:

1. Getting Started
2. F = 0
3. If the bilateral ranks are equal to "1" = the bilateral ranks are equal to "0", then F1 = 1, otherwise F1 = 0.

4. If there is a block of bilateral orders measured by n and there is no gap between the two orders of size, then F2 = 1 or F2 = 0.
5. If there is a gap of the two orders of magnitude n-1 then F3 = 1 or F3 = 0
6. Calculate the function F = F1 + F2 + F3
7. If the result is F = 3, the individual is random, and otherwise the individual is not random, the genetic algorithm will be used.
8. The End.

- Algorithm (3)
  1. Getting Started
  2. Generation of a random generation called the primary generation
  3. Calculate the function of F = Fitness and its order
  4. Find the probability by dividing by the value (Fitness / Fitnesses sum)
  5. Perform the Selection process using a roulette wheel, by randomly generating new ones as well.
  6. Then, crossover process between the new and old generation
  7. Mutation randomly performed on the new generation
  8. A percentage of the old and new generation is chosen according to 40 old to 60 new.
  9. Randomization process of randomization test again on the new generation.
  10. The End
- Algorithm (4)

  A new algorithm has been proposed to hide as follows:
  1. Getting Started
  2. The switch is converted to ASCII coding
  3. It is enclosed within a randomly encoded text
  4. This sequence is written at the end of the ciphertext
  5. The End.

8. The Proposed Algorithm For Decoding

1. Getting Started
2. Receive the encrypted message
3. Approval of the last number to know the number of characters of the original text, which is equal to the number of letters of the key.
4. Depending on the first digits of the first number, the sequence of the key letter and the number of the first number is known.
5. Convert key numbers to binary encoding.
6. Obtaining the flux function is represented by the number that follows the key sequence number.
7. Obtaining the coded text numbers, which are all the remaining numbers.
8. Converting cipher text numbers to binary encoding
9. Decoding the RC4 algorithm
10. Obtain the original express text
11. The End.

9. The Results

1. **Enter the text to be encoded*:*** Initially the text to be encrypted was entered

.

Help Me

Then it was converted to ASCII, then to the dual system, and it became

000101001001010011000100010000010100010000100

After that, the number of bits made up of the text is calculated: No. of bits = 48

2. **Key generation:** The Random Function was used to generate a random number whose length is the length of the text to be encoded after converting to the binary system.

11101011011010110011101110111111010111011011

3. **Random key test:** Two random randomness test keys were constructed, the first function: calculates the number of units and the key beeps and returns the value of F1, zero in the case of zero, equal to 1 or one to one or one to one.

The second function: we enter the value of n, which represents the number of blocks required and was n = 10 and search for n is within the key string and returns the values of zero in the absence of the presence of n in the presence of n in the presence of n. In example, F2 = 0, it also returns either zero in the absence of a n-1 gap or one in the n-1 gap. For example: Fitness = F = F1 + F2 + F3 Fitness = 0. As a result, Objective F is F3 = 0.

Since the value of fitness is not equal to 3, which is an amplification function, we will use the genetic algorithm.

4. **Use the genetic algorithm:**

- Initially, a primary community is generated from individuals. The creation of the primary generation is the starting point. In the solution of the issue, most researchers in this field have indicated that the process of constructing the primary generation is carried out randomly, and is programmatically done by using the (rand) that passes the standard. The one and the number of individuals differ from one issue to another, depending on the type of issue:

10100101111000010000011111110100000010011110100
11101101010111011111111111011110000010011110010
01101000000010011110100101001011110001001110100
01101101010111011111111111011110000010011110010

- Fitness Construction of the Fitness function:

F	no. of chromosomes	F1	F2	F3
0	1	0	0	0
1	2	0	1	0
2	3	0	1	1
1	4	0	1	0

- Building the probability function: This function was built to find the possibility of contributing each of the sections in the following way:

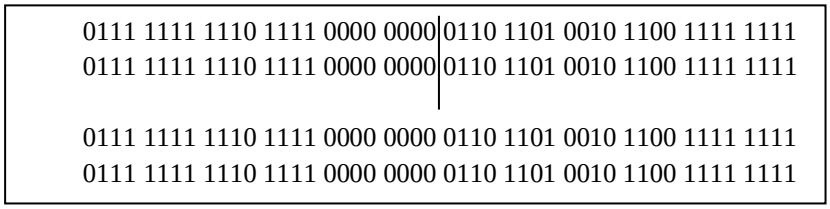
  Pro = Fitness / total Fitness.

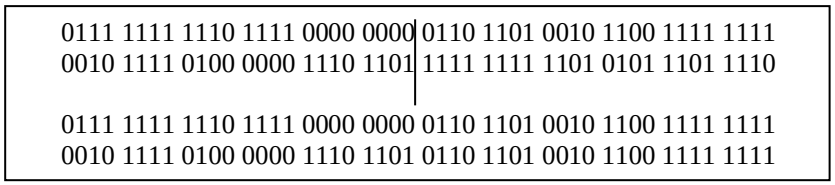
  Pro1 = 2/4 = 1/2 Pro2 = 1/4 Pro3 = 1/4 Pro4 = 0.

- Selection : In this research, the roulette wheel method was chosen to choose individuals from the current generation to produce a new generation. This was done by building *Sel function* to be input to this function matrix representing the pro probability is then generating a matrix of random numbers, and then values compared to the value of each of the random values with the values of the matrix pro use of ready-made function rand, and then create a new matrix *newpro*. Below are the chromosomes that will participate in the marriage process.

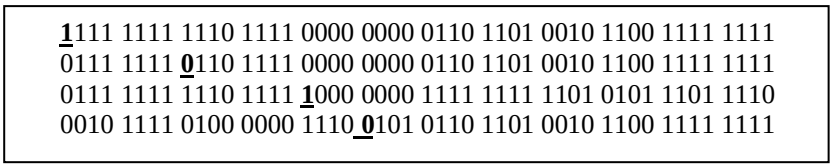
Fitness	No. of chromosomes
2	3
2	3
2	3
1	2

- Crossover Mating : A function has been built to marry after the individuals were selected from the primary generation to have a role in the generation of the next generation, the process of marriage begins through each new two individuals, including This research is relying on simple crossover mating, where a random number was generated and approved as a displacement within the chromosome, at which the interfering (intermarriage) procedure is performed.

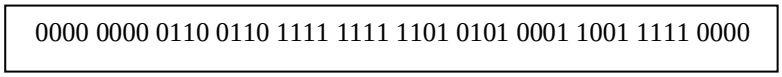




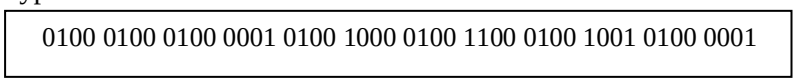
- Mutation: After the marriage process, the role of the mutation in changing the results that result from the marriage process is taken. The mutation ratio is equal to 0.01, and the mutation is represented by forming a ***mut*** function.



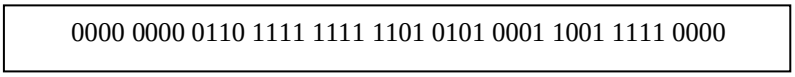
- Evaluating the new generation: After the new generation has been generated, its members are evaluated in the same way as the primary generation.
- Substitution : In this research, a method was adopted that takes into account all members of the generation of both types. Good and bad: 60% of good people and 40% of bad people were taken. Assuming that a chromosome is obtained that matches the state N = 10 and satisfies the functions , F1=1, F2=1, F3 = 1, as follows: F=F1+F2+F3



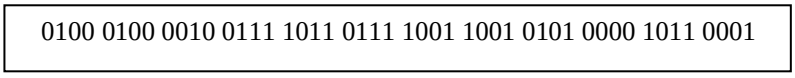
5. **The coding process:** The encoding used is Cipher Stream RC4 as follows:
   - The text to be encrypted:



   - The key used in the encryption process of the camouflage function:



   - The output of the coding process i.e. after the completion of the RC4 process:



6. **Flux function Secure Hash Algorithm (SHA):** After applying the law related to this function, we have the following camouflage function:

   0101 0101

   After converting it, it is equal to 133, after converting the encrypted text, it was as follows:

   68 39 183 153 80 177

   Also, the key after it was converted was in the form:

   00 102 256 213 25 240

In order for the text to be properly encoded and decoded, the coded text has to be available . The key to the recipient of the encrypted message also has the ability to open the encryption, and the key is hidden encoded inside the encrypted message. As a result of the coding, concealment and camouflage function, the text ready for transmission has become the following form, taking into consideration the change in the spaces between the numbers to zero to increase the camouflage:

000102068025602160584970435587865006570430678000345656005402304 50

7. **Decryption :** After receiving the encrypted text and according to the algorithm of decoding the last number represents the number of characters of the text encoded as well as the key which is 6. Also, the key locations are: 10, 8, 4, 3, 1, 0

   It is: 00 102 356 213 25 240

   The camouflage function is 133 to recalculate to verify the reliability of the file being sent, and the original text is: 68 39 183 153 80 177

   After the conversion of the binary system and the XOR process, the result:

   0100 0100 11011 1111 0011 0010 1101 0001 1110 0011 0101 1100

   Then it produces: 68 65 72 76 73 75

   After converting it to the characters, the result was: help me, which is the original text.

8. **Ciphering and decoding time:** The speed of implementation of the coding and coding algorithm was measured to ensure its speed and results. Shown in the following table, given that the program has been applied to a computer with high specifications,

   Labtop acer

   - Intel Celeron M processor 430 (1.73 GHz, 533 MHz FSB, 1 MB L2 cacha)
   - Intel Graphics Media Accelerator 950

The length of the encoding text	Coding Time	Decoding Time
20 character	0.26574	0.12344
40 character	0.254867	0.18675
80 character	0.35044	0.29288
100 character	0.457685	0.38576

We notice from the table above that the coding time for texts and their decoding are good and they are not subject to any rule because the coding of the scripts relies on the key generation process using the genetic algorithm. We also note that the coding time is less than the coding time because in decoding the code is not used genetic algorithm.

10. Conclusions And Recommendations

The proposed method for improving encryption using streamlined encoding has the potential to: Implementation on any computer that has the Matlab system in place, in addition to the difficulty in obtaining cipher key within ciphertext. Also, the proposed method is confidential because of the randomness of the key, which leads to hiding the statistical properties of the express text language and knowing part of the key sequence is not useful in knowing all of the sequences are not repeated as in the known linear and non-linear displacement registers. Therefore, the method has the advantage of being proven in front of a well-known attack (plantext). Other smart technologies can also be used to generate the key, such as the use of neural networks. In addition to the possibility of merging more than one encryption algorithm and utilizing the genetic algorithm by generating key, and use the known flux function which fulfills the specifications required for the flux function MD5.

References

[1] R. V Ericson, *Crime in an insecure world*. Polity, 2007.
[2] D. H. Flaherty, "Protecting privacy in police information systems: data protection in the Canadian Police Information Centre," *Univ. Tor. Law J.*, vol. 36, no. 2, pp. 116–148, 1986.
[3] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, 2011.
[4] E. McFadzean, J. Ezingeard, and D. Birchall, "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Inf. Rev.*, 2007.
[5] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP authentication, authorization, and accounting requirements," *Work Prog.*, 2000.
[6] R. M. Sharma and P. Choudhary, "Synthesis and Simulation of FPGA Based RC4 Encryption Method," *Synthesis (Stuttg).*, vol. 5, no. 4, 2016.
[7] A. A. Alhijaj and M. Kamil Hussein, "Stereo Images Encryption by OSA & RSA Algorithms," *J. Phys. Conf. Ser.*, vol. 1279, no. 1, 2019.
[8] G. S. Basheer, "Application of Polyalphabetic Substitution Cipher using Genetic Algorithm," *AL-Rafidain J. Comput. Sci. Math.*, vol. 5, no. 1, pp. 57–68, 2008.
[9] A. Gorodilov and V. Morozenko, "Genetic Algorithm for finding the Key's length and Cryptanalysis of the Permutation Cipher," 2008.
[10] R. Toemeh and S. Arumugam, "Breaking transposition cipher with genetic algorithm," *Elektron. ir Elektrotechnika*, vol. 79, no. 7, pp. 75–78, 2007.
[11] A. Dimovski and D. Gligoroski, "Attacks on the transposition ciphers using optimization heuristics," *Proc. ICEST*, pp. 1–4, 2003.
[12] M. K. Hussein and A. A. Alhijaj, "TDL and ron rivest, adi shamir and leonard adleman in stereo images encrypt," *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 1 Special Issue, pp. 1811–1817, 2019.
[13] F. J. Kherad, H. R. Naji, M. V Malakooti, and P. Haghighat, "A new symmetric cryptography algorithm to secure e-commerce transactions," in *2010 International Conference on Financial Theory and Engineering*, 2010, pp. 234–237.
[14] A. Maximov, *Some words on cryptanalysis of stream ciphers*. Citeseer, 2006.
[15] D. Eastlake and T. Hansen, "US secure hash algorithms (SHA and HMAC-SHA)." RFC 4634, July, 2006.
[16] R. Patel and N. Chaudhary, "Analyzing Digital Signature Robustness with Message Digest Algorithms," *Comput. Appl. Commun. Secur.*, 2012.
[17] I. Mironov, "Hash functions: Theory, attacks, and applications," *Microsoft Res. Silicon Val. Campus. Noviembre*, 2005.
[18] N. Ferguson *et al.*, "The Skein hash function family," *Submiss. to NIST (round 3)*, vol. 7, no. 7.5, p. 3, 2010.
[19] R. S. McIntyre *et al.*, "Cognitive deficits and functional outcomes in major depressive disorder: determinants, substrates, and treatment interventions," *Depress. Anxiety*, vol. 30, no. 6, pp. 515–527, 2013.
[20] C. Neudecker, N. Mewes, A. K. Reimers, and A. Woll, "Exercise interventions in children and adolescents with ADHD: a systematic review," *J. Atten. Disord.*, vol. 23, no. 4, pp. 307–324, 2019.

Authors

Marwah K. Hussein

Marwah K. Hussein is a lecturer in computer information systems since (2013), University of Basra in Iraq. Her current research interests included information security, Video and image processing.

Kasim Al-Salim

Kasim Alsalim is lecturer in computer science department, faculty of computer science and information technology, university of Basra, Iraq. He completed his BSc and MSc in from university of technology, Baghdad, Iraq. And PhD from the university of Strathclyde, Glasgow, UK. His research field are Distributed Computer Control, Engineering Agents, Smart Meters, Demand-Side Management.

Asaad Alhijaj

Asaad Alhijaj is lecturer in Computer Science and IT College, Basra University, Iraq. He received M.Sc from college of science, Basra university 1994. He also was worked for 9 years ago in Al- Belqaa applied university, Jordan and Al Hussein-bin-Talal university Jordan. His interested in software engineering and Multimedia.

Source details

International Journal of Psychosocial Rehabilitation

Open Access

Scopus coverage years: from 2009 to 2011, from 2013 to Present

Publisher: Hampstead Psychological Associates

ISSN: 1475-7192

Subject area: Psychology: Clinical Psychology | Medicine: Psychiatry and Mental Health | Nursing: Psychiatric Mental Health

View all documents > | Set document alert | Save to source list | Journal Homepage

CiteScore 2018
0.19
Add CiteScore to your site

SJR 2018
0.125

SNIP 2018
0.163

CiteScore | CiteScore rank & trend | CiteScore presets | Scopus content coverage

CiteScore 2018

Calculated using data from 30 April, 2019

$$0.19 = \frac{\text{Citation Count 2018}}{\text{Documents 2015 - 2017*}} = \frac{\text{10 Citations}}{\text{54 Documents}}$$

*CiteScore includes all available document types

View CiteScore methodology > CiteScore FAQ >

CiteScore rank

Category	Rank	Percentile
Psychology — Clinical Psychology	#219/262	16th
Medicine — Psychiatry and Mental Health	#437/494	11th

View CiteScore trends >

CiteScoreTracker 2019

Last updated on *09 April, 2020*
Updated monthly

$$1.03 = \frac{\text{Citation Count 2019}}{\text{Documents 2016 - 2018}} = \frac{\text{98 Citations to date}}{\text{95 Documents to date}}$$

Metrics displaying this icon are compiled according to Snowball Metrics ↗ , a collaboration between industry and academia.

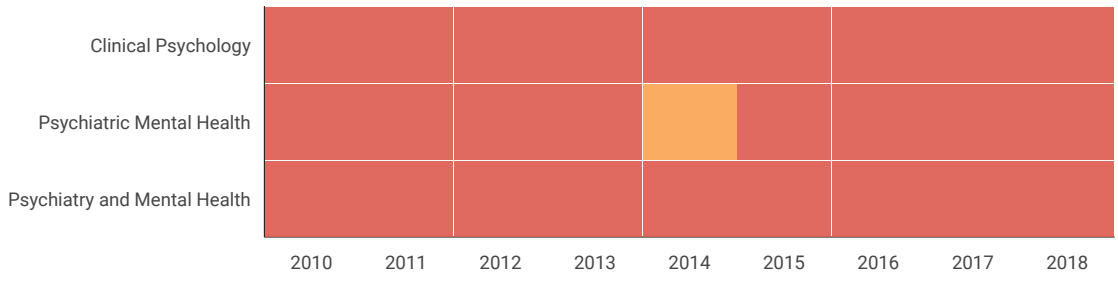
International Journal of Psychosocial Rehabilitation

Country	United Kingdom - SIR Ranking of United Kingdom
Subject Area and Category	Medicine Psychiatry and Mental Health Nursing Psychiatric Mental Health Psychology Clinical Psychology
Publisher	Hampstead Psychological Associates
Publication type	Journals
ISSN	14757192
Coverage	2009-ongoing
Scope	Information not localized
	Homepage How to publish in this journal Contact
	Join the conversation about this journal

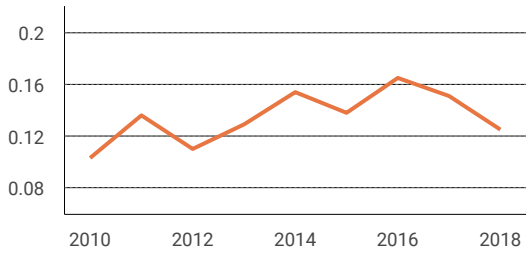
6

H Index

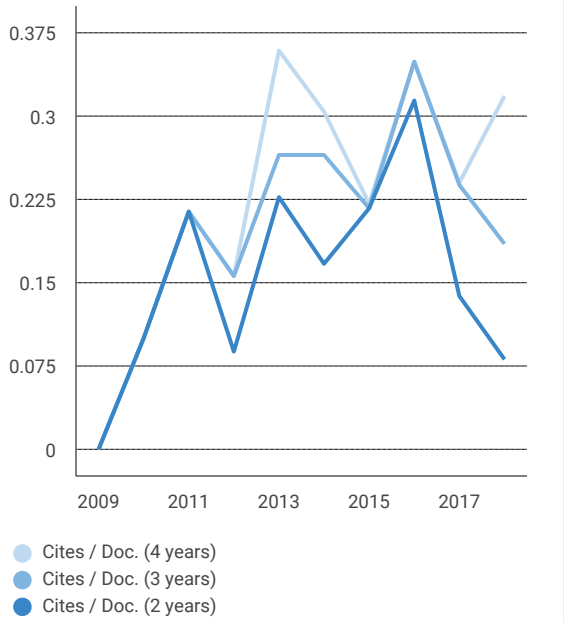
Quartiles



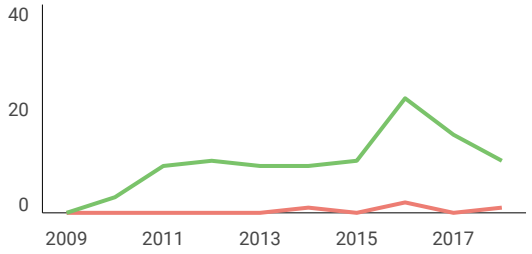
SJR



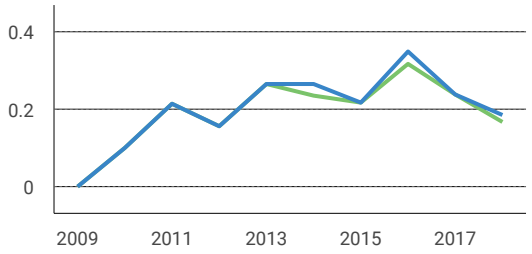
Citations per document



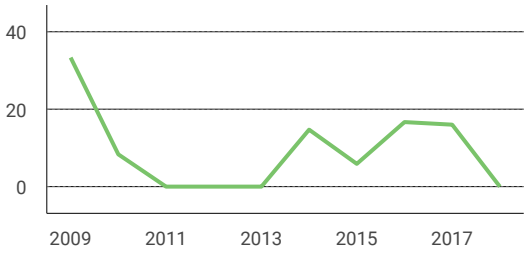
Total Cites Self-Cites



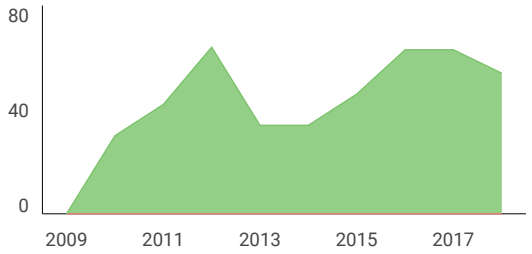
External Cites per Doc Cites per Doc



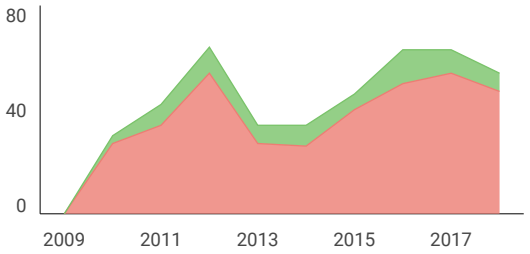
% International Collaboration



Citable documents Non-citable documents



Cited documents Uncited documents



← Show this widget in your own website

Just copy the code below and paste within your html code:

<a href="https://www.scimag

C **CSI A** 35 mins ago

dear sir

i cant open the website for the journal ? any erro on it ?

my regards

reply

M **Minsih** 2 days ago

Dear Chiief Journal

Hallo..Can i get full Article as reference, How to access?

reply

SCImago Team

Melanie Ortiz 2 days ago

Dear Minsih,
thank you for contacting us.
Unfortunately, we cannot help you with your request, we suggest you to contact the journal's editorial staff , so they could inform you more deeply.
Best Regards, SCImago Team

A **Alaa AlDirawi** 3 days ago

Hello team
Please ,can you tell me who much it cost to publish my paper

reply

SCImago Team

Melanie Ortiz 2 days ago

Dear Alaa,
thank you for contacting us.
We are sorry to tell you that SCImago Journal & Country Rank is not a journal. SJR is a

portal with scientometric indicators of journals indexed in Elsevier/Scopus.
Unfortunately, we cannot help you with your request, we suggest you to visit the journal's homepage or contact the journal's editorial staff , so they could inform you more deeply.
Best Regards, SCImago Team

A **Alaa AlDirawi** 3 days ago

i am interest in your journal

reply

H **hatem** 6 days ago

Hello team How much does it cost to publish a research paper in your journal?

reply

SCImago Team

Melanie Ortiz 5 days ago

Dear Hatem,
thank you for contacting us.
We are sorry to tell you that SCImago Journal & Country Rank is not a journal. SJR is a portal with scientometric indicators of journals indexed in Elsevier/Scopus.
Unfortunately, we cannot help you with your request, we suggest you to visit the journal's homepage or contact the journal's editorial staff , so they could inform you more deeply.
Best Regards, SCImago Team

F **Fayza** 6 days ago

Dear Director / International Journal of Psychosocial Rehabilitation
good greeting
Inquire about the cost of publication
How long is the period of publication
What is the classification of the journal q1-2-3
Hope to reply to my inquiry
thank you very much

reply

F **Fayza** 6 days ago

Dear Director / International Journal of Psychosocial Rehabilitation
good greeting
Inquire about the cost of publication
How long is the period of publication
What is the classification of the journal q1-2-3
Hope to reply to my inquiry
thank you very much

reply

Naibaho 2 weeks ago

Dear Scopus,
I would like to know that my manuscript was published already in this Journal at Volume 24 Issue 8 but I don't see the published paper added to the list of my journal in my scopus account. And I try to contact scopus through CHATT but the menu has been deleted from scopus contact.
How could I solve this problem and what should I do?

reply

SCImago Team

Melanie Ortiz 2 weeks ago

Dear Naibaho,
thank you very much for your comment, unfortunately we cannot help you with your request. We suggest you to contact directly with Scopus support:
https://service.elsevier.com/app/answers/detail/a_id/14883/kw/scimago/supporthub/scopus/

Best Regards, SCImago Team

N **Nevi hardika** 2 weeks ago

information is correct whether the title with the author nevi hardika below has been published in your journal (International Journal of Psychosocial Rehabilitation

ISSN: 1475-7192). if it's true how can i download the pdf file. thanks. nevi hardika.

Title:
Manipulative Movement Based on Information Technology Games for School Children Aged 10-12 Years

Authors: Nevi Hardika, Moch. Asmawi, James Tangkudung, Firmansyah Dlis, Achmad Sofyan Hanif, M.E. Winarno, Abdul Sukur, 8Widiastuti
DOI: 10.37200/IJPR/V24I8/PR280033
Pages: 328-339
Keywords: Manipulative Basic Motion Skills, Games, Information Technology.

https://www.psychosocial.com/article-category/issue-8/

reply

SCImago Team

Melanie Ortiz 2 weeks ago

Dear Nevi,
thank you for contacting us.
We are sorry to tell you that SCImago Journal & Country Rank is not a journal. SJR is a portal with scientometric indicators of journals indexed in Elsevier/Scopus.
Unfortunately, we cannot help you with your request, we suggest you contact the journal's

editorial staff , so they could inform you more deeply.
Best Regards, SCImago Team

A **Ali Alqahtani** 3 weeks ago

Is your journal among the Scopus?

reply

SCImago Team

Melanie Ortiz 3 weeks ago

Dear Ali, thank you very much for your comment, unfortunately we cannot help you with your request. We suggest you to consult the Scopus database directly. Keep in mind that the SJR is a static image (the update is made one time per year) of a database (Scopus) which is changing every day.
Best Regards, SCImago Team

F **Fayza** 2 months ago

Dear chief Journal

Hello, My name is Faiza Ahmed and I am following my teacher in special education and autism spectrum disorder. I want to publish a paper in the international journal listed. So anyone please help me with this.
Please send a certified email in order to send the research to the journal
How much is the publication price
Thank you very much in advanc

reply

D **Dr.mustafa Salah** 4 days ago

350$
20-30days publishing

SCImago Team

Melanie Ortiz 2 months ago

Dear Fayza,
thank you for contacting us.
We are sorry to tell you that SCImago Journal & Country Rank is not a journal. SJR is a portal with scientometric indicators of journals indexed in Elsevier/Scopus.
Unfortunately, we cannot help you with your request, we suggest you to visit the journal's homepage (See submission/author guidelines) or contact the journal's editorial staff , so they could inform you more deeply.
Best Regards, SCImago Team

F **Faxriddin A** 2 months ago

do not trust them fake people fake journal they publish all papers what you send just pay

reply

O **oum kumari** 2 months ago

Is this journal still active in Scopus and Scimago (25/2/2020)

reply

SCImago Team

Melanie Ortiz 2 months ago

Dear Oum,
thank you very much for your comment, unfortunately we cannot help you with your request. We suggest you to consult the Scopus database directly. Keep in mind that the SJR is a static image (the update is made one time per year) of a database (Scopus) which is changing every day.
Best Regards, SCImago Team

M **Maher** 2 months ago

I have received this email, is this correct email and is the link below for payment is correct or not:

this is an email i have received:

I am pleased to inform you that your article has been accepted for publication in International Journal of Psychosocial Rehabilitation.

Kindly make payment of 160$ using the below link and send us the receipt

Link: https://secure.payu.in/processInvoice?invoiceId=92060f7615a17a0a47de06b3b86e7756

please please anyone have information tell me.

reply

SCImago Team

Melanie Ortiz 2 months ago

Dear Maher,

thank you for contacting us. Unfortunately, we can not help you with your request, we suggest you to contact the editorial's staff directly. Best regards, SCImago Team

S **suparman Abdullah** 2 months ago

Is this journal still scopus indexed?

reply

SCImago Team

Melanie Ortiz 2 months ago

Dear Suparman, thank you very much for your comment, unfortunately we cannot help you with your request. We suggest you to consult the Scopus database directly. Keep in mind that the SJR is a static image (the update is made one time per year) of a database (Scopus) which is changing every day.
Best Regards, SCImago Team

E **Enda Silvia Putri** 2 months ago

Hello

reply

R **Rajneesh Kumar** 3 months ago

Is "International Journal of Psychosocial Rehabilitation" in the Scopus list in the year 2020?

reply

S **Steffy** 3 months ago

Ma'am,
Is this journal still scopus indexed?

reply

SCImago Team

Melanie Ortiz 3 months ago

Dear Steffy, thank you very much for your comment, unfortunately we cannot help you with your request. We suggest you to consult the Scopus database directly. Keep in mind that the SJR is a static image (the update is made one time per year) of a database (Scopus) which is changing every day.
Best Regards, SCImago Team

D **Dr. Sarab Kadir Mugair** 3 months ago

Dear Sir
Greetings. Plsss let me know asap how can I SMS this journal. I need di Email of journal. Tq

reply

D **Dr M C Jamali** 3 months ago

editor@psychosocial.com

SCImago Team

Melanie Ortiz 2 months ago

Dear user, thanks for your participation! Best Regards, SCImago Team

O **Olga** 3 months ago

Buenas tardes, publique un artículo en la revista, fue aceptado, hice el pago que acordamos, en diciembre vi que fue publicado el artículo pero en este momento la página de la revista fue actualizada y mi artículo no aparece y no me responden de la revista. Que puedo hacer?

reply

SCImago Team

Melanie Ortiz 3 months ago

Dear Olga,
thank you for contacting us.
Sorry to tell you that SCImago Journal & Country Rank is not a journal. SJR is a portal with scientometric indicators of journals indexed in Elsevier/Scopus.
Unfortunately, we cannot help you with your request, we suggest you to contact another member of the journal's editorial staff so they could inform you more deeply. Best Regards, SCImago Team

L **Luma Nasrat Arab** 3 months ago

Good morning sir,madam
I would like to make sure that, is my paper has accepted in your journal please ?
Author name : Luma Nasrat Arab

reply

SCImago Team

Melanie Ortiz 3 months ago

Dear Luma,
thank you for contacting us.
Sorry to tell you that SCImago Journal & Country Rank is not a journal. SJR is a portal with scientometric indicators of journals indexed in Elsevier/Scopus.
Unfortunately, we cannot help you with your request, we suggest you to contact the journal's editorial staff , so they could inform you more deeply. Best Regards, SCImago Team

M **Meenu Sharma** 6 months ago

Hi, my name is Meenu Sharma and i am pursuing my PHD in Psychology. I want to publish a paper in any scopos listed International Journal. So anyone please help me with this. Thanks you so much in advance.

reply

M **Maaza Chaudhary** 3 months ago

Hi, please email me i also have the same issue might be we can help each other or cooperate

M **Methaq** 5 months ago

Send me a message by email

SCImago Team

Melanie Ortiz 6 months ago

Dear Meenu, thanks for your participation! We suggest you to look in the Scopus database to find an indexed journal. Then look the submision guidelines of the journal. Best Regards, SCImago Team

Leave a comment

Name

Email
(will not be published)

I'm not a robot
reCAPTCHA
Privacy - Terms

Submit

The users of Scimago Journal & Country Rank have the possibility to dialogue through comments linked to a specific journal. The purpose is to have a forum in which general doubts about the processes of publication in the journal, experiences and other issues derived from the publication of papers are resolved. For topics on particular articles, maintain the dialogue through the usual channels with your editor.

Developed by: Powered by:

Follow us on @ScimagoJR

Hybrid method for encoding of genetic and RC4 algorithms(بعد التعديلات)

by مروه حسين

Submission date: 10-Apr-2020 10:50AM (UTC+0300)
Submission ID: 1294337321
File name: 6000.pdf (1.11M)
Word count: 4552
Character count: 21930

Hybrid Method For Encoding Of Genetic And RC4 Algorithms

Marwah Kamil Hussein
.University of Basrah, College of Computer Science and Information Technology, Computer Information Systems Dept., Basrah, Iraq
lava85k@gmail.com

Abstract - In this paper, the proposed new method used is to generate the encryption key used in the RC4 algorithm by using the genetic algorithm by randomly generating it using the Rand function, and then subjecting it to the randomized conditions approved. If a match is used for coding, otherwise the genetic algorithm will be used to generate the random genetic key, which is along the length of the text to be encrypted.The proposed method used a new structure to hide the encrypted key within the transferred text, in addition to the integrity of the transferred key (integrity) was confirmed by using a simple flux function.

Keywords- *Coding, RC4, Genetic Algorithms, Voice, Hash Algorithm.*

1. INTRODUCTION

Information security at the world level is an obsession and concern for those in charge of managing various information systems, especially in light of the growing information crime operations that imposed the need for concerted efforts by all countries and governmental and private institutions worldwide, including individuals, to eliminate all violations of information security In particular, in light of the development of technology and the spread of risks involved in its various uses and applications [1].

The term information security is defined in its broad and comprehensive concept as a set of procedures that enables the owner of the information to keep his personal information, data and financial and bank accounts under his full and direct control, and not to allow any unauthorized person to access it with a view to circulating it either in good faith or in bad faith or with the aim of blackmail and tampering It out. Security dysfunctions in information security systems usually occur when the systems are compromised through, for example, hackers, viruses, or any other type of malicious program. Information security professionals strive to ensure the integrity of the various information systems by achieving three basic requirements, which are confidentiality of information, integrity of information, and availability of information [2].

- The fulfillment of the first requirement related to confidentiality of information requires that information be secured in a way that only authorized persons can access it (others with authority or authorized).
- As for the second requirement of confidentiality of information, it seeks to ensure the integrity of the sources of information, so that it cannot be changed or updated only by authorized persons only.
- The third requirement to ensure information security is the possibility and ease of providing information when it is needed. There are also a number of elements that weaken the security systems of different networks and steal information, among which are, for example, password leaks, electronic eavesdropping, hacking, viruses, lures, and identity theft [3][4].

From this standpoint, we know the extreme importance that necessitated the attention of states, governmental and private institutions and individuals, and in light of the development of technology and the spread of risks that have become a problem for societies, technology despite its great services to the human being in the modern era, but it is like any other invention that has many advantages and has serious drawbacks if it does not identify It has to work to avoid it, and in the context of our research we discussed methods and tools to protect the information security of the average user in using the RC4 encryption algorithm [5].

RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code"[6] . The RC4 name is trademark, so RC4 is often referred to as ARCFOUR or ARC4 (this means the alleged RC4) [12] to avoid trademark problems [7].

Noting these advantages, the GA algorithm was used in this research to generate the encryption key used in the RC4 algorithm. After reviewing some previous research that dealt with the uses of GA with coding and decoding, for example: Where researcher [8] has used the genetic algorithm to find the best key to use for encoding texts in a compensatory coding method (Substitution cipher). As for the researcher [9], GA was used to find the length of the secret key that will be used in the analysis of the Permutation cipher. In addition, the search used [10] GA to break the cipher transposition encoded text, and finally researchers [11] introduced three methods of guesswork intuition to reach optimization: (used in the simulation (annealing, genetic algorithm), which was used in the used Transposition cipher [12].

In this research, the genetic algorithm was utilized by proposing a new method for generating the random key used in the RC4 algorithm.

2. STREAM CIPHER OF RC4 ALGORITHM

- Stream cipher operate on a stream of data, one byte at a time.
- Typically stream ciphers perform an Exclusive OR(XOR) operation on a stream of plaintext bytes with the key stream from a pseudo random number generator (PRGA).
- Decryption is achieved by the same byte wise XOR operation on the cipher text.
- Fast and easy to implement in hardware.
- PRGA guidelines:-
  - The key stream must have a large period making the repetition of the a sequence for a part.
  - The key stream generated should possess as much properties as a true random number generator.
  - The input master key (K) must be as a large as possible. [13][14].

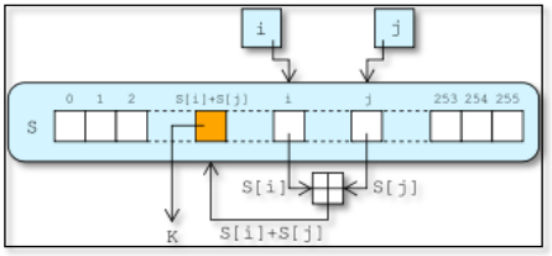


Fig. 1 PRGA flowchart.

3. SCURE HASH ALGORITHM (SHA)

Is one of the Hash algorithms that find a constant string of any text or file, there are several types, including: -

SHA1: This algorithm produces a 160 bit (20 byte) key

SHA512: This algorithm produces a 512 bit (64 byte) key of any message or file of any length and a number of other SHA types as we see it in Figure 4 below and the property of each type. We'll explain in detail how SHA512 works [15][16].

3.1 Part (1):

We know that SHA512 receives any length of data and finds it has a 512 bit HASH length in the Fig. 2. It divides the message into a block each one has a size of 1024 bit and another 128 bit in the last block it is reserved for the length of the real data i.e. this algorithm can find HASH for data with a maximum length of its length 2 ^ 128 and the bits that remain blank between the last 128 bit and the actual data of the message after converting it to binary, we have padding, meaning we enter one number and a number of zeros follow it until we fill in the empty bits. And the last block accepts only 896 bits because as we said the last 128 bits in the last block are reserved for the length of the real message in binary system format where iv = H0 represents the eight registers (A, B, C, D, E, F, G, H) each one of its size 64 bit total is 512 bit which will eventually represent the message's Hash. These are initial values stored within Registers. See Fig. 2 [17].

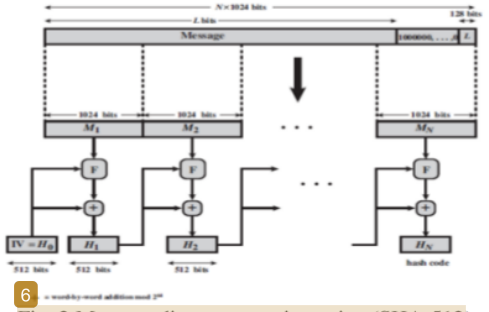


Fig. 2.Message digest generation using (SHA-512).

3.2 Part (2):

Which represents Part 2 in the Fig. 2 is the letter (F) in Part No. 1, where it repeats its same operations with each block so we will explain on one Block and the rest of the same thing. Fig.3 represents the operations that will be performed on each

block of the real message to produce a key whose length is 512 bits stored in (A, B, C, D, E, F, G, H) and is considered as an entry for operations on the next Block if the data is more than Block As shown in Fig. 3, or the final result is considered if the data is a single block. And that each (F) is divided into 80 Round, each one carrying out the operations inside him once (Part 4 in Fig. 5 represents the operations that will take place within each Round) . In the Fig. 3, each round of 80 is entered with a value of a certain K between (K0-K79), which are fixed values consisting of 64 bits taken from the following table [17].

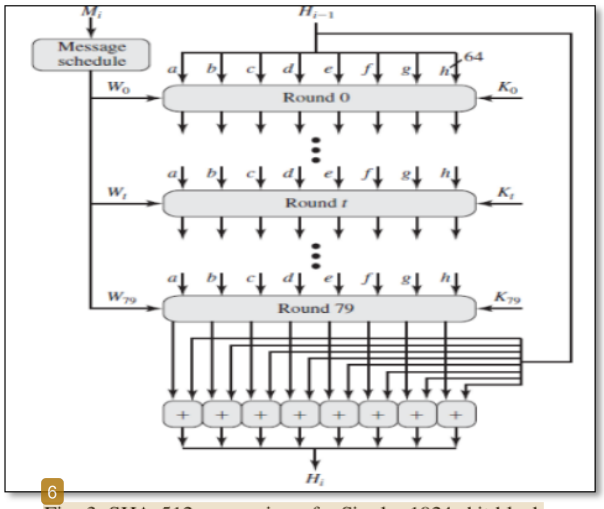


Fig. 3. SHA-512 processing of a Single 1024- bit block.

3.3 Part (3):

We also note that in the Fig. 4, each Round enters a value from Block data of 64 bit length and that the length of one Block is 1024 bit, so it divides (1024) into 16 Block, each one of which is 64 bit size represented (W0-W15) and enters the first 16 Round and the rest of Round takes Wt according to the following formula [18].

$$W_t = \sigma_1^{512}(W_{t-2}) + W_{t-7} + \sigma_0^{512}(W_{t-15}) + W_{t-16}$$

where

$$\sigma_0^{512}(x) = ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x)$$

$$\sigma_1^{512}(x) = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^6(x)$$

$ROTR^n(x)$ = circular right shift (rotation) of the 64-bit argument x by n bits

$SHR^n(x)$ = left shift of the 64-bit argument x by n bits with padding by zeros on the right.

+ = addition modulo 2^{64}

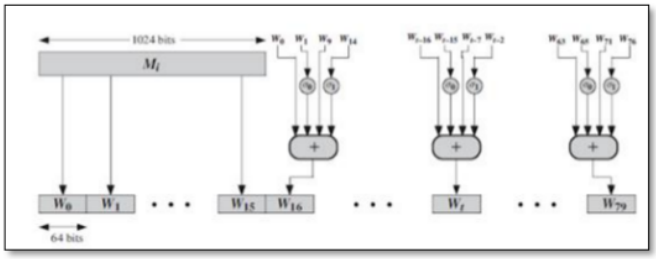


Fig. 4. Creation of 80-word input Sequence for SHA-512 processing of single block.

3.4 Part (4):

Part No. 4 in Fig. 5 represents the operations that will take place within each Round in order to not update them on the Registers values that will consider the updated values as the next Round entry and in the last Round is the Hash of the message if the message is from one block and otherwise it is considered an entry for Registers data in the next Block W_t Block: represents 64 bit of Block data previously explained in preparation for each Round [18].

K_t: These are 64-bit constant values taken from the table previously explained

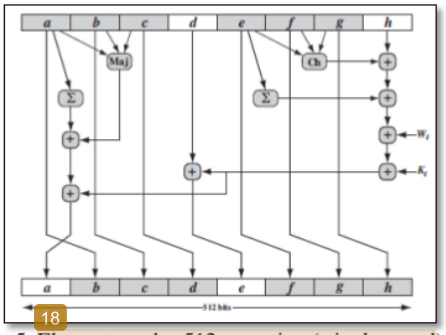


Fig. 5. Elementary sha-512 operation (single round).

$$T_2 = (\sum_0^{512} a) + Maj(a, b, c)$$

$h = g$, $g = f$, $f = e$, $e = d + T_1$, $d = c$, $c = b$, $b = a$, $a = T_1 + T_2$

where

t = step number, $0 \leq t \leq 79$

$$Ch\ (e,f,g) = (e\ AND\ f)\ \oplus\ (NOT\ e\ AND\ g)$$

The conditional function: If e then f else g

$$Maj\ (a,b,c) = (a\ AND\ b) \oplus (a\ AND\ c) \oplus (b\ AND\ c)$$

The function is true only of the majority (two or three) of the arguments are true

$$(\sum_0^{512} a\ ) = \text{ROTR}^{28}\ (a) \oplus \text{ROTR}^{34}\ (a) \oplus \text{ROTR}^{39}\ (a)$$

$$(\sum_1^{512} a) = \text{ROTR}^{14}\ (e) \oplus \text{ROTR}^{18}\ (e) \oplus \text{ROTR}^{41}\ (e)$$

ROTR^n (x) = circular right shift (rotation) of the 64-bit argument x by n bits

W_t = a 64-bit word derived from the current 512-bit input block

K_t = a 64-bit additive constant

4. GENERAL STEPS OF THE GENETIC ALGORITHM:

- Create a primary generation
- Find the function of the objective, the extent of fitness, and the potential contribution to the primary generation
- Sections
- Parent test (Selection).
- Interventional intervention (Crossover)
- Change within one syllable (Mutation)
- Standard for stopping the genetic algorithm [19][20]

5. RESEARCH OBJECTIVE

To obtain more confidentiality, faster implementation and less cost, an algorithm was proposed. Hybrids take advantage of the genetic characteristics to make a key and check its randomness by using approved methods. Instead of regenerating the key at the receiving end, a new method has been used to hide the key. Inside the encoded text before sending, the integrity of the received key has been confirmed by using the SHA camouflage function.

6. SUGGESTED WAY TO CONFIGURE THE KEY:

Genetic algorithm has been relied upon to avoid behaviors caused by the traditional method. In Initially, a random generation of key is generated using the rand function in Matlab, noting that the length of the key must be the length of the text to be encoded, and then the tribe is measured from the randomness. As per the approved conditions [5], if the conditions are fulfilled, the individual is random and will be used for coding. The whole primary generation does not fulfill the conditions the genetic algorithm is used.

7. STRUCTURE OF THE PROPOSED METHOD:

The basis for successful encryption is the approved algorithm and key confidentiality. The following algorithm has been adopted:

- *Algorithm (1)*
  1. Getting Started
  2. Enter the express text to be encrypted
  3. Convert the express text to the binary code using the ASCII code. 4. Calculate the number of bits in which the text is made after converting it to the binary system. 5. The code is shown in the code with the code.
  4. Random Key Test According to Algorithm (2)
  5. In the event that it does not fulfill the conditions of the algorithm (2), the genetic algorithm (3) is used.
  6. If the conditions are met, the key is used to encode the express text using the RC4 encoding method.
  7. SHA Flux Calculation for the key and result set at end of text after encoding
  8. Hide the key within ciphertext according to algorithm (4(
  9. Calculate the number of characters of the original text and place it at the end of the text
  10. Send the message
  11. End.
- *Algorithm (2).*

The approved conditions were used to randomize the test [5] as follows:

1. Getting Started
2. F = 0
3. If the bilateral ranks are equal to "1" = the bilateral ranks are equal to "0", then F1 = 1, otherwise F1 = 0.
4. If there is a block of bilateral orders measured by n and there is no gap between the two orders of size, then F2 = 1 or F2 = 0.
5. If there is a gap of the two orders of magnitude n-1 then F3 = 1 or F3 = 0
6. Calculate the function F = F1 + F2 + F3
7. If the result is F = 3, the individual is random, and otherwise the individual is not random, the genetic algorithm will be used.
8. The End.

- Algorithm (3)
  1. Getting Started
  2. Generation of a random generation called the primary generation
  3. Calculate the function of F = Fitness and its order
  4. Find the probability by dividing by the value (Fitness / Fitnesses sum)
  5. Perform the Selection process using a roulette wheel, by randomly generating new ones as well.
  6. Then, crossover process between the new and old generation
  7. Mutation randomly performed on the new generation
  8. A percentage of the old and new generation is chosen according to 40 old to 60 new.
  9. Randomization process of randomization test again on the new generation.
  10. The End
- Algorithm (4)

  A new algorithm has been proposed to hide as follows:
  1. Getting Started
  2. The switch is converted to ASCII coding
  3. It is enclosed within a randomly encoded text
  4. This sequence is written at the end of the ciphertext
  5. The End.

8. THE PROPOSED ALGORITHM FOR DECODING

1. Getting Started
2. Receive the encrypted message
3. Approval of the last number to know the number of characters of the original text, which is equal to the number of letters of the key.
4. Depending on the first digits of the first number, the sequence of the key letter and the number of the first number is known.
5. Convert key numbers to binary encoding.

6. Obtaining the flux function is represented by the number that follows the key sequence number.
7. Obtaining the coded text numbers, which are all the remaining numbers.
8. Converting cipher text numbers to binary encoding
9. Decoding the RC4 algorithm
10. Obtain the original express text
11. The End.

9. THE RESULTS

1. **Enter the text to be encoded:** Initially the text to be encrypted was entered

Help Me

Then it was converted to ASCII, then to the dual system, and it became

000101001001010011000100010000010100010000100

After that, the number of bits made up of the text is calculated: No. of bits = 48

2. **Key generation:** The Random Function was used to generate a random number whose length is the length of the text to be encoded after converting to the binary system.

111010110110101100111011101111101011101110 11

3. **Random key test:** Two random randomness test keys were constructed, the first function: calculates the number of units and the key beeps and returns the value of F1, zero in the case of zero, equal to 1 or one to one or one to one.

The second function: we enter the value of n, which represents the number of blocks required and was n = 10 and search for n is within the key string and returns the values of zero in the absence of the presence of n in the presence of n in the presence of n. In example, F2 = 0, it also returns either zero in the absence of a n-1 gap or one in the n-1 gap. For example: Fitness = F = F1 + F2 + F3 Fitness = 0. As a result, Objective F is F3 = 0.

Since the value of fitness is not equal to 3, which is an amplification function, we will use the genetic algorithm.

4. Use the genetic algorithm:

- Initially, a primary community is generated from individuals. The creation of the primary generation is the starting point. In the solution of the issue, most researchers in this field have indicated that the process of constructing the primary generation is carried out randomly, and is programmatically done by using the (rand) that passes the standard.

The one and the number of individuals differ from one issue to another, depending on the type of issue:

1010010111000010000011111110100000001001111010 0
1110110101011101111111111110111100000010011110010
0110100000001001111010010100101111000100111101 00
0110110101011101111111111110111100000010011110010

- Fitness Construction of the Fitness function:

F	no. of chromosomes	F1	F2	F3
0	1	0	0	0
1	2	0	1	0
2	3	0	1	1
1	4	0	1	0

- Building the probability function: This function was built to find the possibility of contributing each of the sections in the following way:

  Pro = Fitness / total Fitness.

  Pro1 = 2/4 = 1/2 Pro2 = 1/4 Pro3 = 1/4 Pro4 = 0.

- Selection : In this research, the roulette wheel method was chosen to choose individuals from the current generation to produce a new generation. This was done by building *Sel function* to be input to this function matrix representing the pro probability is then generating a matrix of random numbers, and then values compared to the value of each of the random values with the values of the matrix pro use of ready-made function rand, and then create a new matrix *newpro*. Below are the chromosomes that will participate in the marriage process.

Fitness	**No. of chromosomes**
2	3
2	3
2	3
1	2

- Crossover Mating : A function has been built to marry after the individuals were selected from the primary generation to have a role in the generation of the next generation, the process of marriage begins through each new two individuals, including This research is relying on simple crossover mating, where a random number was generated and approved as a displacement within the chromosome, at which the interfering (intermarriage) procedure is performed.

0111 1111 1110 1111 0000 0000 | 0110 1101 0010 1100 1111 1111
0111 1111 1110 1111 0000 0000 | 0110 1101 0010 1100 1111 1111

0111 1111 1110 1111 0000 0000 0110 1101 0010 1100 1111 1111
0111 1111 1110 1111 0000 0000 0110 1101 0010 1100 1111 1111

0111 1111 1110 1111 0000 0000 | 0110 1101 0010 1100 1111 1111
0010 1111 0100 0000 1110 1101 | 1111 1111 1101 0101 1101 1110

0111 1111 1110 1111 0000 0000 0110 1101 0010 1100 1111 1111
0010 1111 0100 0000 1110 1101 0110 1101 0010 1100 1111 1111

- Mutation: After the marriage process, the role of the mutation in changing the results that result from the marriage process is taken. The mutation ratio is equal to 0.01, and the mutation is represented by forming a ***mut*** function.

1111 1111 1110 1111 0000 0000 0110 1101 0010 1100 1111 1111
0111 1111 **0**110 1111 0000 0000 0110 1101 0010 1100 1111 1111
0111 1111 1110 1111 **1**000 0000 1111 1111 1101 0101 1101 1110
0010 1111 0100 0000 1110 **0**101 0110 1101 0010 1100 1111 1111

- Evaluating the new generation: After the new generation has been generated, its members are evaluated in the same way as the primary generation.
- Substitution : In this research, a method was adopted that takes into account all members of the generation of both types. Good and bad: 60% of good people and 40% of bad people were taken. Assuming that a chromosome is obtained that matches the state N = 10 and satisfies the functions , F1=1, F2=1, F3 = 1, as follows: F=F1+F2+F3

0000 0000 0110 0110 1111 1111 1101 0101 0001 1001 1111 0000

5. **The coding process:** The encoding used is Cipher Stream RC4 as follows:
   - The text to be encrypted:

0100 0100 0100 0001 0100 1000 0100 1100 0100 1001 0100 0001

   - The key used in the encryption process of the camouflage function:

0000 0000 0110 1111 1111 1101 0101 0001 1001 1111 0000

- The output of the coding process i.e. after the completion of the RC4 process:

0100 0100 0010 0111 1011 0111 1001 1001 0101 0000 1011 0001

6. **Flux function Secure Hash Algorithm (SHA):** After applying the law related to this function, we have the following camouflage function:

0101 0101

After converting it, it is equal to 133, after converting the encrypted text, it was as follows:

68 39 183 153 80 177

Also, the key after it was converted was in the form:

00 102 256 213 25 240

In order for the text to be properly encoded and decoded, the coded text has to be available . The key to the recipient of the encrypted message also has the ability to open the encryption, and the key is hidden encoded inside the encrypted message. As a result of the coding, concealment and camouflage function, the text ready for transmission has become the following form, taking into consideration the change in the spaces between the numbers to zero to increase the camouflage:

000102068025602160584970435587865006570430678000345656005402304 50

7. **Decryption :** After receiving the encrypted text and according to the algorithm of decoding the last number represents the number of characters of the text encoded as well as the key which is 6. Also, the key locations are:

10, 8, 4, 3, 1, 0

It is: 00 102 356 213 25 240

The camouflage function is 133 to recalculate to verify the reliability of the file being sent, and the original text is

68 39 183 153 80 177

After the conversion of the binary system and the XOR process, the result:

0100 0100 11011 1111 0011 0010 1101 0001 1110 0011 0101 1100

Then it produces: 68 65 72 76 73 75

After converting it to the characters, the result was: help me, which is the original text.

8. **Ciphering and decoding time:** The speed of implementation of the coding and coding algorithm was measured to ensure its speed and results. Shown in the following table, given that the program has been applied to a computer with high specifications,

Lab acer

- Intel Celeron M processor 430 (1.73 GHz, 533 MHz FSB, 1 MB L2 cacha)
- Intel Graphics Media Accelerator 950

The length of the encoding text	Coding Time	Decoding Time
20 character	0.26574	0.12344
40 character	0.254867	0.18675
80 character	0.35044	0.29288
100 character	0.457685	0.38576

We notice from the table above that the coding time for texts and their decoding are good and they are not subject to any rule because the coding of the scripts relies on the key generation process using the genetic algorithm. We also note that the coding time is less than the coding time because in decoding the code is not used genetic algorithm.

10. CONCLUSIONS AND RECOMMENDATIONS

The proposed method for improving encryption using streamlined encoding has the potential to:

Implementation on any computer that has the Matlab system in place, in addition to the difficulty in obtaining cipher key within ciphertext. Also, the proposed method is confidential because of the randomness of the key, which leads to hiding the statistical properties of the express text language and knowing part of the key sequence is not useful in knowing all of the sequences are not repeated as in the known linear and non-linear displacement registers. Therefore, the method has the advantage of being proven in front of a well-known attack (plantext). Other smart technologies can also be used to generate the key, such as the use of neural networks. In addition to the possibility of merging more than one encryption algorithm and utilizing the genetic algorithm by generating key, and use the known flux function which fulfills the specifications required for the flux function MD5.

References

[1] R. V Ericson, *Crime in an insecure world*. Polity, 2007.

[2] D. H. Flaherty, "Protecting privacy in police information systems: data protection in the Canadian Police Information Centre," *Univ. Tor. Law J.*, vol. 36, no. 2, pp. 116–148, 1986.

[3] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, 2011.

[4] E. McFadzean, J. Ezingeard, and D. Birchall, "Perception of risk and the strategic impact of existing IT on information security strategy at board level," *Online Inf. Rev.*, 2007.

[5] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP authentication, authorization, and accounting requirements," *Work Prog.*, 2000.

[6] R. M. Sharma and P. Choudhary, "Synthesis and Simulation of FPGA Based RC4 Encryption Method," *Synthesis (Stuttg).*, vol. 5, no. 4, 2016.

[7] A. A. Alhijaj and M. Kamil Hussein, "Stereo Images Encryption by OSA & RSA Algorithms," *J. Phys. Conf. Ser.*, vol. 1279, no. 1, 2019.

[8] G. S. Basheer, "Application of Polyalphabetic Substitution Cipher using Genetic Algorithm," *AL-Rafidain J. Comput. Sci. Math.*, vol. 5, no. 1, pp. 57–68, 2008.

[9] A. Gorodilov and V. Morozenko, "Genetic Algorithm for finding the Key's length and Cryptanalysis of the Permutation Cipher," 2008.

[10] R. Toemeh and S. Arumugam, "Breaking transposition cipher with genetic algorithm," *Elektron. ir Elektrotechnika*, vol. 79, no. 7, pp. 75–78, 2007.

[11] A. Dimovski and D. Gligoroski, "Attacks on the transposition ciphers using optimization heuristics," *Proc. ICEST*, pp. 1–4, 2003.

[12] M. K. Hussein and A. A. Alhijaj, "TDL and ron rivest, adi shamir and leonard adleman in stereo images encrypt," *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 1 Special Issue, pp. 1811–1817, 2019.

[13] F. J. Kherad, H. R. Naji, M. V Malakooti, and P. Haghighat, "A new symmetric cryptography algorithm to secure e-commerce transactions," in *2010 International Conference on Financial Theory and Engineering*, 2010, pp. 234–237.

[14] A. Maximov, *Some words on cryptanalysis of stream ciphers*. Citeseer, 2006.

[15] D. Eastlake and T. Hansen, "US secure hash algorithms (SHA and HMAC-SHA)." RFC 4634, July, 2006.

[16] R. Patel and N. Chaudhary, "Analyzing Digital Signature Robustness with Message Digest Algorithms," *Comput. Appl. Commun. Secur.*, 2012.

[17] I. Mironov, "Hash functions: Theory, attacks, and applications," *Microsoft Res. Silicon Val. Campus. Noviembre*, 2005.

[18] N. Ferguson *et al.*, "The Skein hash function family," *Submiss. to NIST (round 3)*, vol. 7, no. 7.5, p. 3, 2010.

[19] R. S. McIntyre *et al.*, "Cognitive deficits and functional outcomes in major depressive disorder: determinants, substrates, and treatment interventions," *Depress. Anxiety*, vol. 30, no. 6, pp. 515–527, 2013.

[20] C. Neudecker, N. Mewes, A. K. Reimers, and A. Woll, "Exercise interventions in children and adolescents with ADHD: a systematic review," *J. Atten. Disord.*, vol. 23, no. 4, pp. 307–324, 2019.

Hybrid method for encoding of genetic and RC4 algorithms(بعد التعديلات)

ORIGINALITY REPORT

15%	8%	5%	13%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to An-Najah National University Student Paper	4%
2	Submitted to Kingston University Student Paper	3%
3	Submitted to The University of Manchester Student Paper	2%
4	Submitted to CSU, San Jose State University Student Paper	1%
5	en.wikipedia.org Internet Source	1%
6	Neha Agrawal, Bhale Pradeepkumar, Shashikala Tapaswi. "Preventing ARP spoofing in WLAN using SHA-512", 2013 IEEE International Conference on Computational Intelligence and Computing Research, 2013 Publication	1%
7	Submitted to Legacy High School Student Paper	1%

8	www.scribd.com Internet Source	<1%
9	www.xtron.sk Internet Source	<1%
10	datatracker.ietf.org Internet Source	<1%
11	Submitted to The Robert Gordon University Student Paper	<1%
12	www.87994.com Internet Source	<1%
13	wingsman2.mine.nu Internet Source	<1%
14	Submitted to Misr International University Student Paper	<1%
15	fr.scribd.com Internet Source	<1%
16	Isaac De L. Oliveira Filho, Otaciana G.R. Santiago, Anne M.P. Canuto, Benjamin R.C. Bedregal. "A Comparative Analysis of Cryptographic Algorithms and Transformation Functions for Biometric Data", 2013 12th International Conference on Machine Learning and Applications, 2013 Publication	<1%

17	trac.ietf.org Internet Source	<1%
18	Submitted to University of Westminster Student Paper	<1%

Exclude quotes	Off	Exclude matches	< 3 words
Exclude bibliography	On		