# A Robust Approach for Mixed Technique of Data Encryption Between DES and RC4 Algorithm

**Tameem Hameed Obaida**
Al-Furat Alawsat Technical University
Najaf Technical Institute
Computer systems department
Email: tameem_hameed @ yahoo . com

**Dhafar Hamed Abd**
Al Maaref University College
Department of Computer Science
Email:dhafar.dhafar@Gmail.com

.

## Abstract

In this research, the well-known encryption algorithms in the encryption Systems, namely DES & RC4 and the advantages and disadvantages of each algorithm are reviewed and evaluated. These two algorithms are combined to produce of new algorithm which is more efficient unscrambling due to the increasing of the level of complexity that make it highly resistance to several attacks. The new algorithm is implemented to show its efficiency in term of time complexity, (i.e. Breaking the code will be much more complicated than if it would have been occurring through the use of each algorithm individually), this process can be achieved with a very small time difference (approximately neglected in the encryption process). When this algorithm is applied and tested in practice the following result has been obtained:

When a block is encrypted using the DES algorithm, the time spent may be (0.000034) milliseconds, but when using the new algorithm to encrypt the same block, the time taken will be about (0.000042) milliseconds. To encrypt 1024 blocks using the DES algorithm, it will take a time of (0.0406),while by using the new algorithm the time taken for encryption is only (0.051). This gives very little increase in time compared to increasing of complexity obtained. Since the new algorithm combining from the two previous, ones allows us to encrypt each block with a key differs from the other one (i.e. each block is encrypted with a different key depending on the preceding block), making it very difficult to break the code leading to an increase in security and information protection against decoding.

**Keywords:** RC4, DES, combined DES & RC4,combined Approach, Data Encryption, complexity.

## الخلاصة

تم في هذا البحث استعراض خوارزميات التشفير المعروفة في أنظمة التشفير وهما خوارزميتي RC4 &DES وبيان سلبيات وايجابيات كل خوارزمية ، ثم تم دمج الخوارزميتين بخوارزمية واحدة للحصول على خوارزمية أكثر كفاءة من خلال زيادة نسبة التعقيد للخوارزمية الجديدة الناتجة (أي عملية كسر الشفرة ستكون اعقد بكثير مما لو تم استخدام كل خوارزمية على حده) وبفرق قليل (مهمل) في الوقت المستغرق في عملية التشفير. بعد تطبيق الخوارزمية الجديدة واختبارها عمليا تم الحصول على النتيجة التالية :-

عند تشفير بلوك واحد باستخدام خوارزمية الـ DES سيكون الوقت المستغرق للتشفير هو( 0.000034) ملي ثانية إما عند استخدام الخوارزمية الجديدة لتشفير نفس البلوك سوف يكون الوقت المستغرق بالتشفير هو (0.000042)، ولتشفير 1024 بلوك باستخدام خوارزمية الـ DES سوف تستغرق وقت مقداره (0.0406) إما باستخدام الخوارزمية الجديدة سيكون الوقت المستغرق للتشفير هو (0.051) . وهذا يعطي زيادة قليلة جدا في الوقت مقارنة مع زيادة نسبة التعقيد التي تم الحصول عليها، حيث إن الخوارزمية الجديدة الناتجة من دمج الخوارزميتين السابقتين تتيح لنا تشفير كل بلوك بمفتاح يختلف عن البلوك الأخر (أي كل بلوك يُشفر بمفتاح مختلف يتم توليده بالاعتماد على البلوك السابق) يعني صعوبة كبيرة في كسر الشفرة وهذا يقودنا إلى زيادة في الأمنية وحماية المعلومات من الاختراق.

## 1. Introduction:

The large and vast development in networks and computers and social media and applications that interconnect people among each other lead to huge growth and exchanging of data and information related to persons and institutions. Thus there is an intense need is generated to secure these data and information against illegal access except for some authorized persons. As a result, programmers have done their best either to design new algorithms or develop some of available ones to encrypt messages and exchanged texts or to

increase their encryption complexion levels to make it more complex to be decrypted [1-2]. Previously there were some algorithms of interest such as DES used to protect the information in U.S.A., which is considered as a complex one since it uses a 64-bit, from which only 56 bits are used for cyphering while the other bits are used for error checking [3].

This algorithm uses a dependent-on-secrete key cyphering, and this is why this algorithm can be broken and hacked later on. Many trials were performed to increase the security level of an algorithm through increasing of its complexity level. One of these trials was the issuing of "Triple DES" algorithm, which means using of DES three times with a different key each time. Some researchers had developed a new algorithm, RC4 which was the first in using the general key of length of 1024 bits in expectation and encryption giving then algorithm an extra strength to be broken and revealed. It was an important step during that time. The researchers continued to develop their works. Such as William Stallings in his book "Cryptography and Network Security", S. Kruti and B. Gambhava in their book "New Approach of Data Encryption Standard Algorithm" and S. Singh in "Performance Analysis of DES and RSA Cryptography", in addition to other researchers worked and still searching about developing and analysis of new highly secure algorithms. This work is focusing on combining the two different algorithms (DES & RC4) each of them works in an independent different method in one combined more complex code which will be discussed in details through this work [7].

The purpose of encryption is to achieve the security which are Confidentiality , Integrity, Authentication and Non-Repudiation. and Which represent objectives of encryption .And there are two types of cryptography, first, Symmetric Cryptography: This type of encryption is a conventional where the same key is used for encryption and decryption such that when the key is known, the message will be easily read and understood. DES method is some examples of this type, second, Asymmetric Cryptography , In this type, two keys are used, public and private, where the public one is used for encryption, it can be publicly sent or given for encryption. The private is kept by the owner only to be used in decryption of the message. The following are some examples about the public key, DSA, Deffie-Hellman, RSA [8].

Also the strength scale of encryption algorithms depend on time it must be kept as minimum as possible in both encryption and decryption processes. and Complexity It must be as maximum as possible to make it very hard to the unauthorized to decrypt the ciphertext of the messages [4-5].

## 2. Algorithm Description

Due to the disadvantages referred to above in DES & RC4, a new algorithm is designed combining advantages of both DES & RC4 to avoiding their disadvantages and deficiencies. In this work the two algorithms mentioned above are combined together in one code, such that RC4 is inserted in the right part of DES directed left wise through the interchange process[6] .

We know how "DES " algorithm encrypts a block of 64 bit by dividing it into two parts left and right where each part occupies 32bit. By this work, the left side of "DES" algorithm is made to act according to its own principle, while the right one acts as an "RC4" algorithm. This technique makes the resulting algorithm more complex and unbreakable by any attack. The time taken for encryption and decryption is as little as that of "DES" or nearly close to it.

Following a flowchart illustrated in figure (1) showing the combination process between (DES & RC4) algorithms.

As it is clearly seen in the chart that the key is inserted in the RC4 algorithm located at the right part i.e. making an "XOR" on both the message bits and the key, then the second key is obtained which later on will be inserted in RC4 algorithm again and so on till finishing all stages of DES algorithm completely. Thus the resulting code will be very complex and unbreakable.

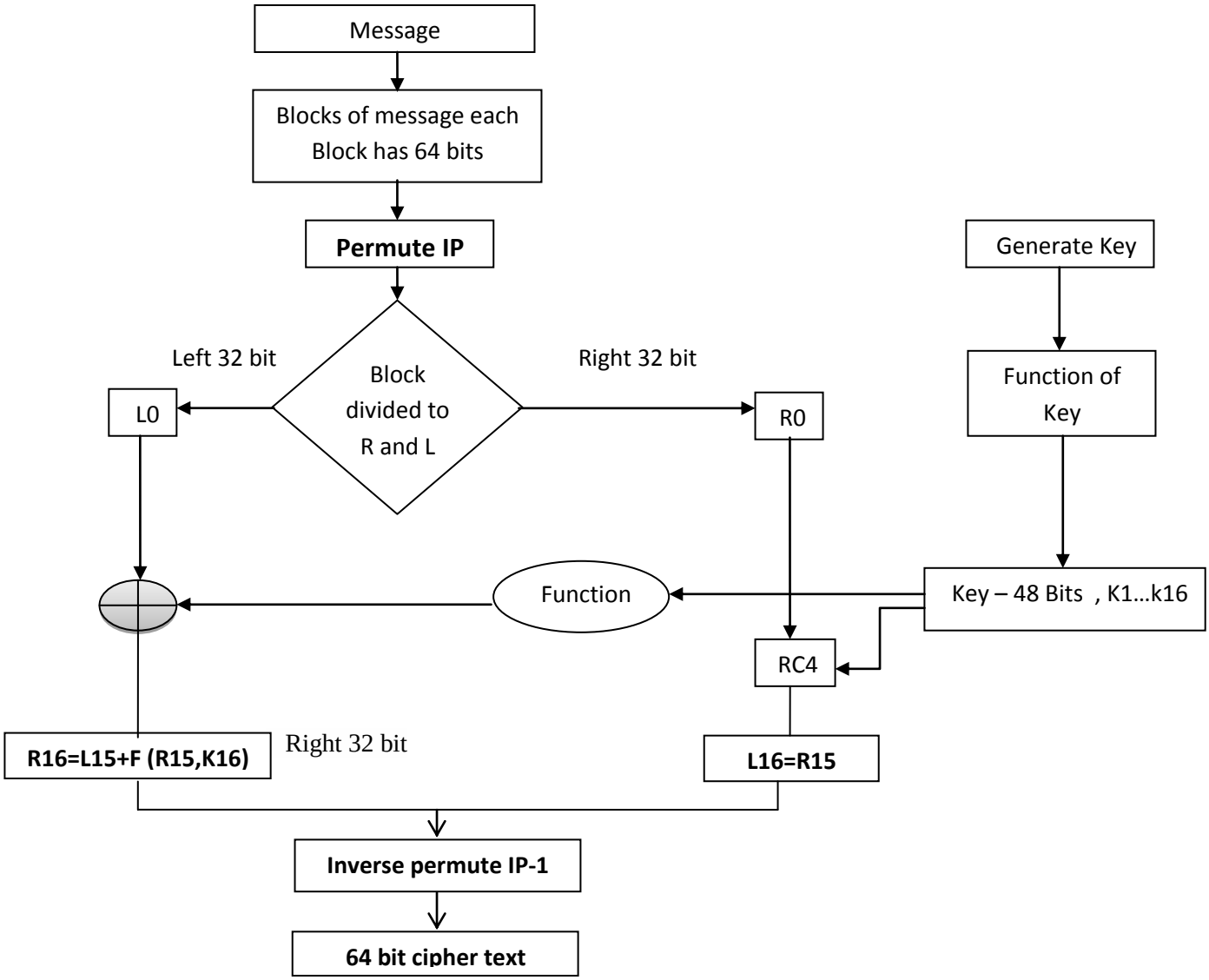


**Figure 1: Flowchart to Explain Combining (DES & RC4)**

The following chart in figure (2) is showing how to insert RC4 algorithm working by stream cipher with DES algorithm working by Block cipher.

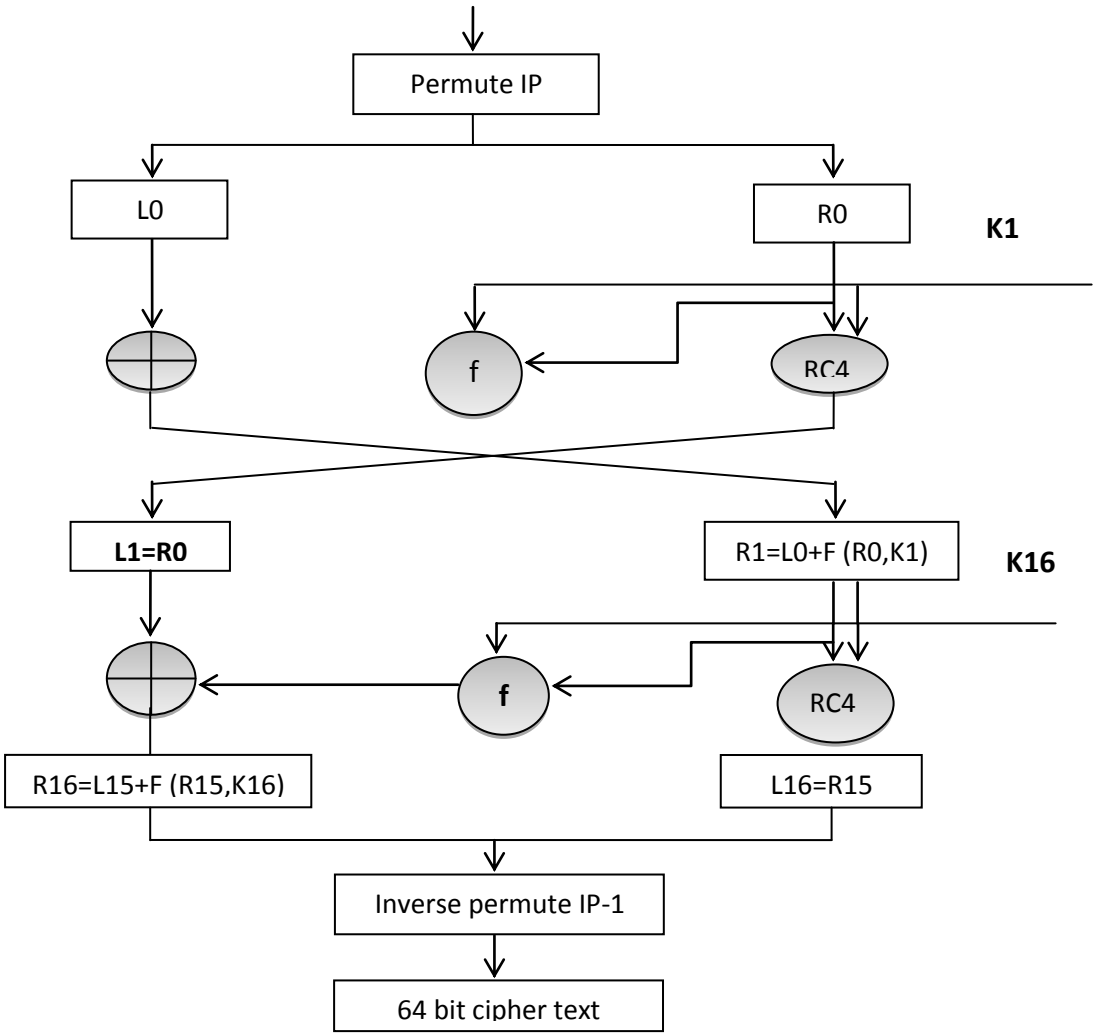


**Figure 2: Flowchart to Add RC4 for DES steps.**

The algorithm of this flowchart is shown below:

## Notation

To simplify our discussion, we can use the following variables:

$\sum$ is the alphabet that we are using, with $\sum^*$ is our language.

ei is a character in the alphabet **S = { e0, e1, e2, ... en-1 }.**

T is our encryption transformation (algorithm).

K is the set of all possible keys (key space).

k is the key we choose to use $k \in K$.

M is our plaintext message $M \in S^*$.

mi a character (sometimes referred to as a block) in the plaintext M**. M = { m0, m1, ... }.**

C is the resulting ciphertext $C = T_k ( M )$.

ci a character (also referred to as a block) in the cipher C. **C = { c0, c1, ... }**

Any cipher can expressed as the following function $C = T_k ( M )$ and alternatively $M = T_k^{-1} ( C )$.

## Pseudo code

Input to process

1- Message.
2-convert message to HEX where
Hexadecimal base 16.
3- Convert Hex to Binary where base 64-bit.

## Processing

1-the following pseudo-code shows how it DES is often implemented in software.

```
Function DES_Encrypt (M, K) where M = (L, R).
        M ← IP(M)

   For  round ← 1  to  16  do
      Ki ← SK (K , round)
      L ← RC4 (R ,  Ki)
      L ← L XOR F(R, Ki)
      swap (L,  R)
         end
   Swap (L, R)
   M ← IP-1  (M)
   return M
  end.
```

2- The algorithm for decrypting is similar. The only difference is the order in which the keys are used.

```
Function DES_Decrypt (C, K)    where  C     = (L, R)
   C ← IP (C)
   for round ← 16  to  1  do
      Ki ← SK (K, round)
     L ← RC4 (R,  Ki)
      L  ← L XOR  F(R,  Ki)
      swap (L, R)
   end
   swap (L,  R)
   C ← IP-1(C)
   return C
   end.
```

## 3. Results and Discussion

The new algorithm is applied using "visual Basic.net 2010". A comparison between the results obtained from it and those obtained from "DES" gives the differences in time taken as shown in table-1.

**Table (1): Explain Time Rates**.

| Number of Block | DES only | DES with RC4 |
|---|---|---|
| 4 | 0.00034 | 0.00042 |
| 8 | 0.00062 | 0.00078 |
| 16 | 0.0012 | 0.0016 |
| 32 | 0.0020 | 0.0027 |
| 64 | 0.0034 | 0.0049 |
| 128 | 0.0068 | 0.0088 |
| 256 | 0.0118 | 0.0159 |
| 512 | 0.0230 | 0.0297 |
| 1024 | 0.0406 | 0.051 |

Note: All the opened applications in the computer are closed in order to compute the time consumed as .much accurate as possible.

It is noted that in table-1 that the time taken in encryption of 4 blocks by "DES" method only is "0.00034" while by the combined code is "0.00042" Following is a flowchart showing the combination process between (DES & RC4) algorithms.

As it has been the representation of the difference in time between DES and RC4 algorithms in the following chart. Figure (3).

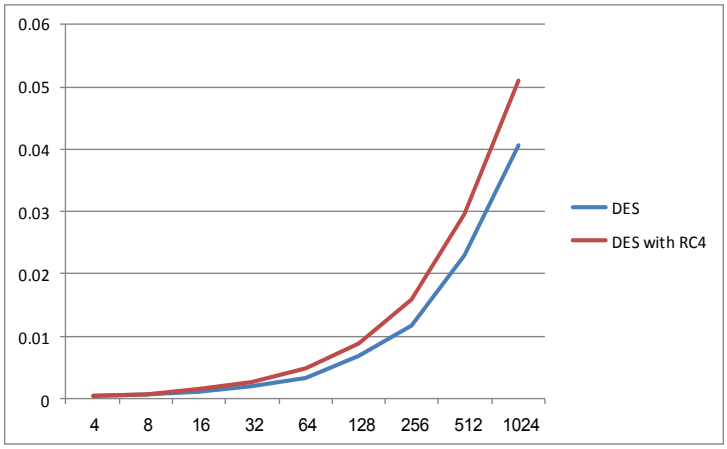


**Figure 3: Difference in Time (DES & RC4)**

Then the complexity of the DES algorithm is computed based on the length text required to be encoded.

The following equation is then used after divide it to a number of single blocks.

**Complexity=(64! * 16 Round)**

Where: (64): represents the length of the block required to be encoded..

(16): represents the no. of cyphering cycles of 64-bit.

However, to compute the complexity of new developed algorithm, the equation is consider.

**Complexity =(64! * 32! * 32 Round)*16 Round**

Where: (64): represents the length of the block required to be encoded..

(32!): represents the size of half of the block entered from the right-hand side using RC4 algorithm.

(32): represents the no. of cyphering cycles of half of the block entered from the right-hand side using RC4 algorithm, considering that this choice depends on key size, because this algorithm works with a no. of cycles of a length of 256, while the entered key here has a length of only of 32.

The following example illustrates the number of different bits with real-time, where the message "welcome to" was taken, and converted to a number of

bilateral bits. A 64-bit-size-block from these bits was taken and encrypted with the DES algorithm only and then,

encrypted again (same text) by the new algorithm resulting from merging process and recording the time taken for each of them, the results obtained are as stated in the following table (2):

**Table (2): plaintext encryption with (DES&RC4).**

| Message | Block1 | DES with RC4 | Time |
|---|---|---|---|
| welcome to | 1 1 1 0 1 1 1 0 1 0 1 0 0 1 1 0 0 0 1 1 0 1 1 0 1 1 0 0 0 1 1 0 1 1 1 1 0 1 1 0 1 0 1 1 0 1 1 0 0 0 0 0 0 1 0 0 0 0 1 0 1 1 1 0 | 1 0 0 1 1 1 1 1 1 1 0 0 1 0 0 1 1 0 1 1 0 0 1 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 1 1 0 0 0 1 1 1 0 0 0 0 1 0 0 0 0 0 0 1 0 0 1 0 0 | 0.000578 |
| | | **DES** | |
| | | 0 0 0 1 1 1 0 1 0 0 1 1 0 1 1 1 0 1 0 1 0 1 1 1 0 1 1 1 1 0 1 1 0 1 1 0 0 1 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 1 1 1 1 0 1 1 0 1 0 1 | 0.000398 |

## 4. Conclusion

We conclude from this research it is possible to take advantage of the well-known encryption algorithms, through combined them (combine two or more algorithms in one algorithm) and product new algorithms more strength and durability in data encryption and this in order to increase the proportion of the complexity of the code-breaking operation.

## 5. References:

[1] W. Stallings, 2005, "THE RC4 STREAM ENCRYPTIION ALGORIITHM", Available online at www.IEEE.com.

[2] A. Mousa, and A. Hamad, 2006, "Evaluation of the RC4 Algorithm for Data Encryption", International journal of computer sciences and applications.

[3] A. .Jeeva, V. Palanisamy, and K. Kanagaram, 2012, "COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND SECURITY MEASURES OF SOME ENCRYPTION ALGORITHMS ",

International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.3033-3037.

[4] Q. Galvane and B. Uzel, 2012, "Cryptography - RC4 Algorithm".

[5] L. Stošić and M. Bogdanović, 2012, "RC4 stream cipher and possible attacks on WEP", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012.

[6] S. Kruti and B. Gambhava, 2012, "New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March.

[7] S. Singh, S. K. Maakar and S. Kumar, 2013, "A Performance Analysis of DES and RSA Cryptography", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org, Volume 2, Issue 3, May–June 2013 ISSN 2278-6856.

[8] D. and B. Kapoor, 2014, "State of the Art Realistic Cryptographic Approaches for RC4 Symmetric Stream Cipher", International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.4, DOI:10.5121/ijcsa.2014.4403, Department of Computer Science Engineering, Chitkara University, Himachal Pradesh, India.