Iraqi Journal of Science, 2024, Vol. 65, No. 6, pp: 3434-3450
DOI: 10.24996/ijs.2024.65.6.37

Multilevel Cryptography Model using RC5, Twofish, and Modified Serpent Algorithms

Mays M. Hoobi
Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

Received: 11/1/2023 Accepted: 25/5/2023 Published: 30/6/2024

Abstract

Due to the rapid development of digital communication systems, information security is now essential for both the storage and exchange of data. Security has become a key research axis as a result of the rapid evolution of network technologies. The transmission of digital data is necessary for various forms of communication. Particularly in applications requiring a high level of security, like surveillance applications, military applications, biometric applications, and radar applications, where this transmission should be secure. Thus, data is normally encoded through the technique of encryption to prevent unauthorized access. The current imperative is for cyber security to guarantees the integrity and confidentiality of data transmission over the internet and offer defense against hostile attacks. To ensure the security and dependability of digital data transmission, the goal of this research is to create and analyze a robust multilevel cryptography model using three cases. Those cases include: case 1 utilized the RC5 algorithm only. Case 2 examined the use of RC5 together with the Twofish algorithms, and case 3 employed a combination of three effective algorithms in sequential order (RC5 with Twofish and Modified Serpent). The results were analyzed and showed that case 3—which encrypts data by applying three effective algorithms sequentially—is preferable. This case offers a performance model for various combinations of the symmetric key cryptography algorithms RC5, Twofish, and modified Serpent. Utilizing analysis tools including entropy, floating frequency, histogram, autocorrelation, and brute force attack, the three cases were compared.

Keywords: Block Cipher, Cryptography, Modified Serpent, RC5, Twofish.

نموذج تشفير متعدد المستويات باستخدام خوارزميات *RC5* و *Twofish* و *Serpent* المعدلة

ميس محمد هوبي

قسم علوم الحاسوب، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة

نظرًا للتطور السريع لأنظمة الاتصالات الرقمية، أصبح أمن المعلومات الآن ضروريًا لتخزين البيانات وتبادلها. يصبح الأمان محور بحث رئيسي نتيجة للتطور السريع لتقنيات الشبكة. يعد نقل البيانات الرقمية ضروريًا لمختلف أشكال الاتصال. يجب أن يكون هذا الإرسال آمنًا، لا سيما في التطبيقات التي تتطلب مستوى عالٍ من الأمان، مثل تطبيقات المراقبة والتطبيقات العسكرية وتطبيقات القياسات الحيوية وتطبيقات

Email: mays.m@sc.uobaghdad.edu.iq

الرادار. يتم تشفير البيانات من خلال تقنية التشفير لمنع الوصول غير المصرح به. الضرورة الحالية هي للأمن السيبراني، والذي يضمن سلامة وسرية نقل البيانات عبر الإنترنت ويوفر دفاعًا ضد الهجمات العدائية. من أجل ضمان أمن وموثوقية نقل البيانات الرقمية، فإن الهدف من هذا البحث هو إنشاء وتحليل نموذج تشفير قوي متعدد المستويات باستخدام حالات ثلاث مختلفة. تتضمن هذه الحالات الحالة 1 التي تستخدم ببساطة خوارزمية RC5 ، والحالة 2 باستخدام RC5 مع خوارزميات Twofish ، والحالة 3 التي تستخدم مزيجًا من ثلاث خوارزميات فعالة بترتيب تسلسلي (RC5 مع Twofish و Serpent المعدل). يتم تحليل النتائج وتبين أن الحالة 3 – التي تقوم بتشفير البيانات عن طريق تطبيق ثلاث خوارزميات فعالة بالتتابع – هي الأفضل. تقدم هذه الحالة نموذج أداء لمجموعات مختلفة من خوارزميات تشفير المفتاح المتماثل RC5 و Twofish و Serpent المعدل. تقدم هذه الحالة نموذج أداء لمجموعات مختلفة من خوارزميات تشفير المفتاح المتماثل RC5 و Twofish و Serpent المعدل. باستخدام أدوات التحليل بما في ذلك الانتروبيا، والتردد العائم ، والمدرج التكراري ، والارتباط التلقائي ، وهجوم القوة الوحشية ، تمت مقارنة ثلاث حالات.

1-Introduction

The science of cryptology, which mostly relies on mathematics, is concerned with the scientific foundations of such methods (cryptanalysis and cryptography). A crucial step in ensuring security in multimedia systems is encryption [1]. In a number of industries, including medical imaging, online communications, military communications, and multimedia systems, image and video encryption is important. The confidentiality of multimedia data is the main goal. For ensuring the data's security, the encryption process converts the data into a code. The plaintext (original message prior to encryption) is subjected to different transformations and substitutions by encryption algorithms, which turn it into ciphertext (scrambled message following encryption). As seen in Figure 1, decryption is a technique for converting encrypted data back into plaintext [2].

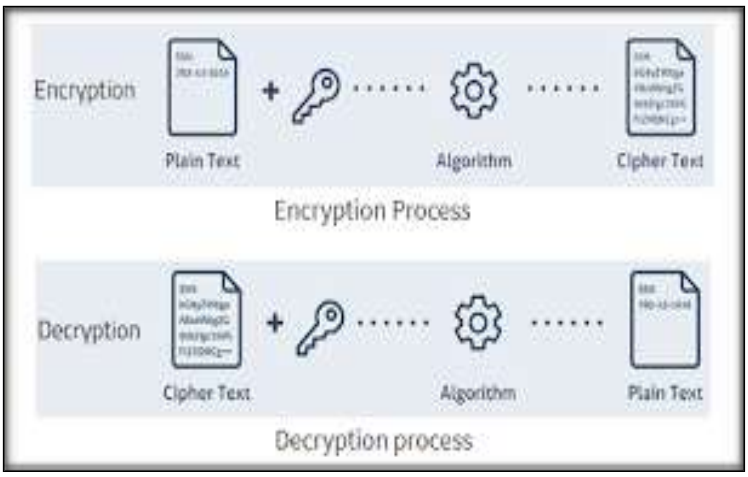


Figure 1: Encryption and Decryption Processes[2]

Symmetric (secret-key) and Asymmetric (public-key) encryption are two classes that are used for classifying cryptography algorithms. Various symmetric-key block ciphers provide varying degrees of security, adaptability, and effectiveness. The symmetric-key block ciphers that have attracted the most interest among the various ones currently in use include RC5, DES, Blowfish, CAST, SAFER, FEAL, and IDEA. A Feistel network construction and round function provide the foundation of the majority of symmetric-key block ciphers, including RC5, DES, Blowfish, and CAST. Through combining numerous straightforward nonlinear

and linear operations including substitution, exclusive-or, modular arithmetic, and permutation, the round function offers a fundamental encryption technique. Various round functions offer varying degrees of security, effectiveness, and adaptability [3].

The3436his3436nning sections of this research are organized to include related work in section2, then sections 3,4, and 5 respectively clarify the basics of the algorithms used in this research. Section 6 explains the tools that were used to analyze the results of the proposed system. Section 7 presents the proposed system with different cases. The last two sections introduce the results discussion and conclusions consequently.

2- Related Work:

The efficiency improvement of the cryptographic algorithms was the aim of numerous research, some of which are listed in this section:

In [4], cryptography was defined as a key part in the information security of the current world that makes the virtual world a safe place. If possible, the users require cryptographic algorithms to be the low-cost as well as have high-performance. In this study, the researchers performed a thorough analysis of costs and performance of some of the main cryptographic approaches (such as the AES, Blowfish, DES, 3-DES, and RSA) to show overall performance analyses, different from the mere theoretical comparison.

The authors of [5] proposed merging 2 effective algorithms of encryption to satisfy information security by adding a new level of security to 3-DES using N-th Degree Truncated Polynomial Ring Unit method. Such objective was accomplished by the addition of two new key functions, the first was Enc_key (), and the second the Dec_key (). Those were used for the encryption and decryption key of the 3-DES to the increase of algorithm strength. The results that was obtained in this paper shows very good resistance towards brute-force attacks This results in increasing system efficiency with the use of the abovementioned algorithm for the encryption and decryption of 3-DES key, since such modifications enhance the level of complexity, and increase key search space, in addition to making encrypted message difficult to crack by any attacker.

In [6], the authors assumed the combination of 2 sufficient encryption algorithms to achieve the objective of information security by adding a new level of the security to the DES algorithm through using elliptic curve method. Results that were obtained from this study demonstrated a sufficient resistance to brute-force attacks, which makes this system of a greater effectiveness through applying elliptic curve cryptography approach for the encryption and decryption of keys with the use of the DES. Additionally, those modifications lead to improving the complexity degree and increasing the key search space.

In [7], their work resulted in the increase in RSA’s complexity and search space against brute force attacks. Also, security enhancements were satisfied through the application of four cases with the use of various cryptographic algorithms. Those four cases included case1 enhancement if RSA security with the use of the OAEP (i.e. Optimal Asymmetric Encryption Padding), case2 the combination of the two most significant methods Diffie-Hellman (DH) and RSA, case3 in order to increase the complexity and obtain higher security level the two cases above (case 1 and case 2) were concatenated. Lastly, for maximum complexity and to obtain the highest level of security with increasing RSA’s search space case 4 was implemented. Case 4 included implementing case 3 as well as applying new security level through the addition of another cryptographic algorithm, which was referred to as the HiSea. The use of multiple cryptographic algorithms in every one of the 4 cases above respectively resulted in the improvement of the security level through the increase in complexity and key

search space which results in protecting the security goals against attackers. Case 4 was the optimal scenario since it presents most sufficient, accurate, and complex encryption system that utilizes the processing of the encryption data several times with the use of various strong algorithms.

3- RC5 Algorithm

A symmetric block cipher called RC5 was created with both hardware and software implementation in mind. It can be defined as a parameterized algorithm that has a variable size of the block, a variable key length, and variable number of the rounds. This offers a chance for significant flexibility in the properties of the performance and security levels. One specific version of the RC-5 algorithm is known as RC5-w/r/b. The w parameter in RC5 refers to the word size in bits. Various selections for this parameter provide various RC5 methods. With the variable number of rounds, the RC5 has an iterative arrangement. The 2nd parameter of the RC5 is the quantity of rounds, or r. A variable-length secret key is utilized by the RC5 algorithm . Finally, ® 3rd parameter is the length of the key, which is specified in bytes. The following is a summary of the parameters [8]:

***1- w*: word size, in bits**. has a standard value of 32bits. Permissible values include 16, 32 and 64. RC5 performs the encryption of 2-word blocks so that plain-text and blocks of cipher-text are 2*w* bits long each.

***2- r*: number of rounds.** Its permissible values are in the range of 0, 1,..., 255. In addition to that, expanded key table *S* includes $t = 2(r + 1)$ words.

3- b*: represents number of the bytes in secret key *K. its permissible values are in the range of 0, 1,..., 255. *K*: *b*-byte secret key; *K*[0], *K*[1],.., *K*–*b* − 1]

RC5 has 3 components, which are: an algorithm of key expansion, an encryption and a decryption algorithms.

Input block to the algorithm of RC5 includes 2 *w*-bit words, given in 2 registers, which are referred to as *A* and *B*. The output is placed in registers *A* and *B*. As mentioned earlier, the RC5 utilizes expanded key table, *S*[0, 1,. .,–*t* − 1], which consists of $t = 2(r + 1)$ words. The algorithm of the key-expansion initializes *S* from user's given secret key parameter *K*. On the other hand, *the S table* in the RC5 encryption isn't like the S-box that has been utilized by the DES. The steps of the encryption and decryption of the RC5 are described below in algorithms 1 and 2[9]:

Algorithm1: (RC5 Encryption Algorithm)

***Step1: A* += *S*[0]**

***Step2: B* += *S*[1]**

Step3: f®r *i* = 1 to *r*

***A* = ((*A* ⊕ *B*) <<< *B*) + *S* [2 *i*]**

***B* = ((*B* ⊕ *A*) <<< *A*) + *S* [2 *i* + 1]**

The output is in *A* and *B* registers

Algorithm2: (RC5 Decryption Algorithm)

Step1: ®or *i* = *r* down to 1 do

B* = ((*B* – ® [2 *i* + 1]) >>> *A*) ⊕ *A

A* = ((*A* – *S* [2 *i*]) >>> *B*) ⊕ *B

***Step2:* – = *B* − *S*[1]**

***Step3:* – = *A* − *S*[0]**

The routine of decryption may be derived easily from the routine of the encryption. RC5 encryption/decryption algorithms are depicted in Figures 2 and 3 respectively [9].

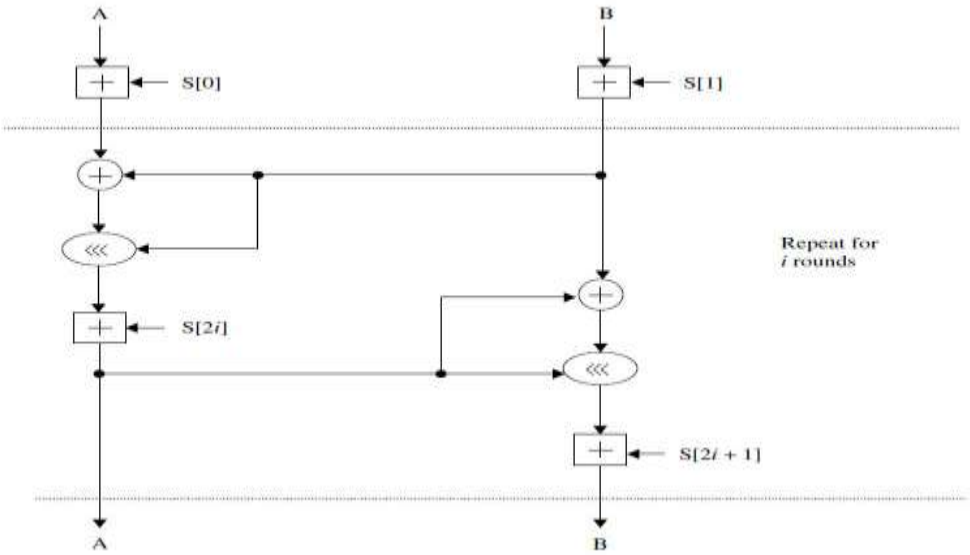


Figure 2: RC5 Encryption Algorithm[9]

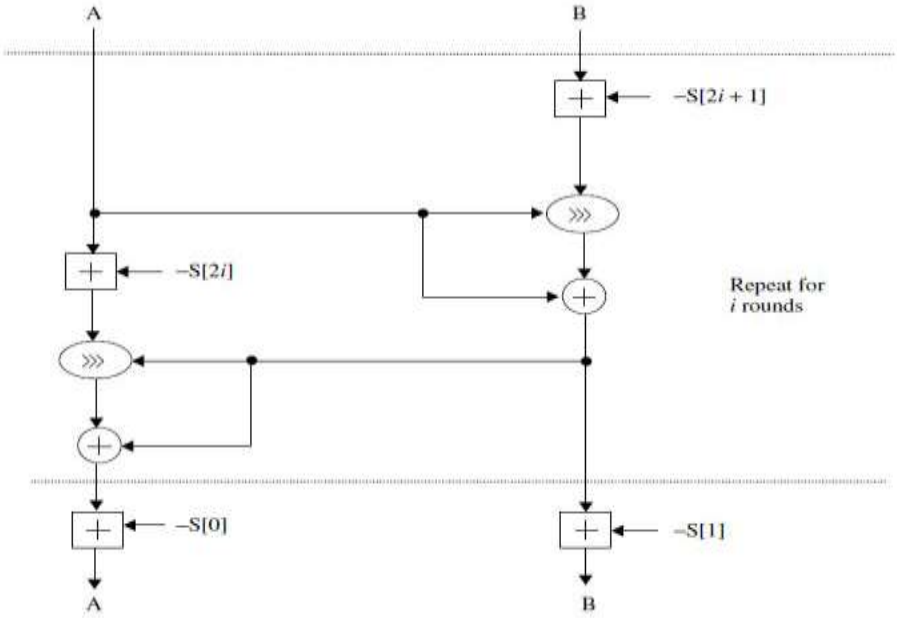


Figure 3: RC5 Decryption Algorithm [9]

4-Twofish Algorithm

Block cipher Twofish, which was submitted alongside AES and made it to the c'ntest's finals, was never taken into consideration for standardization. With a Feistel structure key to DES and a block size of 128 bits that can be expanded to 256 bits. The fundamental components of Twofish are four separate key-dependent 8x8-bit S-boxes, 16 rounds of Feistel networks, Maximum Distance Separable (MDS) matrices, and the concepts of key whitening and key scheduling. An iterated block 'ipher's security can be increased using the key whitening approach in cryptography [10].

It includes procedures for combining the data with a component of the key. An algorithm known as a key schedule determines all the round keys from the key. There are no weak keys, as for a 128-bit symmetric block cipher, keys have lengths of 128, 192, and 256 bits, and a 128-bit key length. See Figure 4 for other examples [11].

Algorithm 3: (Twofish algorithm)
Step1: divide input bit to 4 parts.
Step2: perform XOR operation between bit input with a key.
Step3: processing input bits in 16 times Feistel network.
Twofish algorithm is more secure in comparison to other algorithms with no cryptanalysis yet to be found possible.

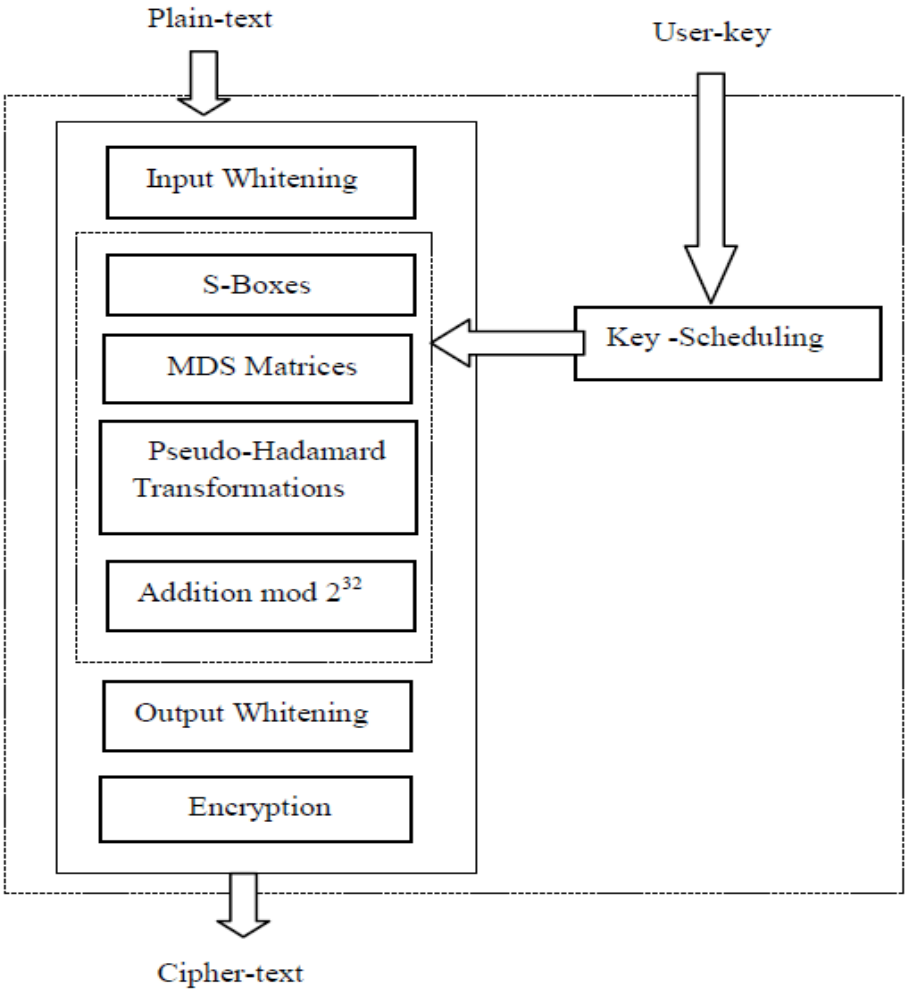


Figure 4: Twofish Algorithm Structure[11]

5- Serpent Algoithm

One of the top candidates for a new block cipher using the AES was the serpent encryption algorithm. They created the Serpent block cipher, along with Knudsen and Biham. Despite having a relatively conservative design, it can nonetheless be implemented quite effectively. It employs S-boxes like those in DES in a novel structure that simultaneously permits a faster avalanche, a more effective bit slice implementation, and an easier analysis that shows its security against all known attack types[12].

Any characteristic should have a minimum of one active S-box in each round in Serpent, which uses a 256-bit key and a 128-bit block size. Due to the feature that a deference in only one bit in the input creates a deference of at least two bits in each S-output', at least two active S-boxes are often needed. As a result, if only one bit in the input of one round differs, at least two bits must also differ in the output, and these two bits affect two different S-boxes in the subsequent round, the output variations affect at least four S-boxes in the subsequent

round. As shown in Figure 5, Serpent algorithm runs via a 32-Round substitution permutation network that operates on a 4 × 32-bit length. A 128-bit plain-text is encrypted in 32 rounds and then Xor with 33 subkeys to produce a 128-bit ciphertext. Users are thought to enter a variable key length, yet in reality, it is anticipated that a fixed length of 128, 192, or 256 bits would be used[13].

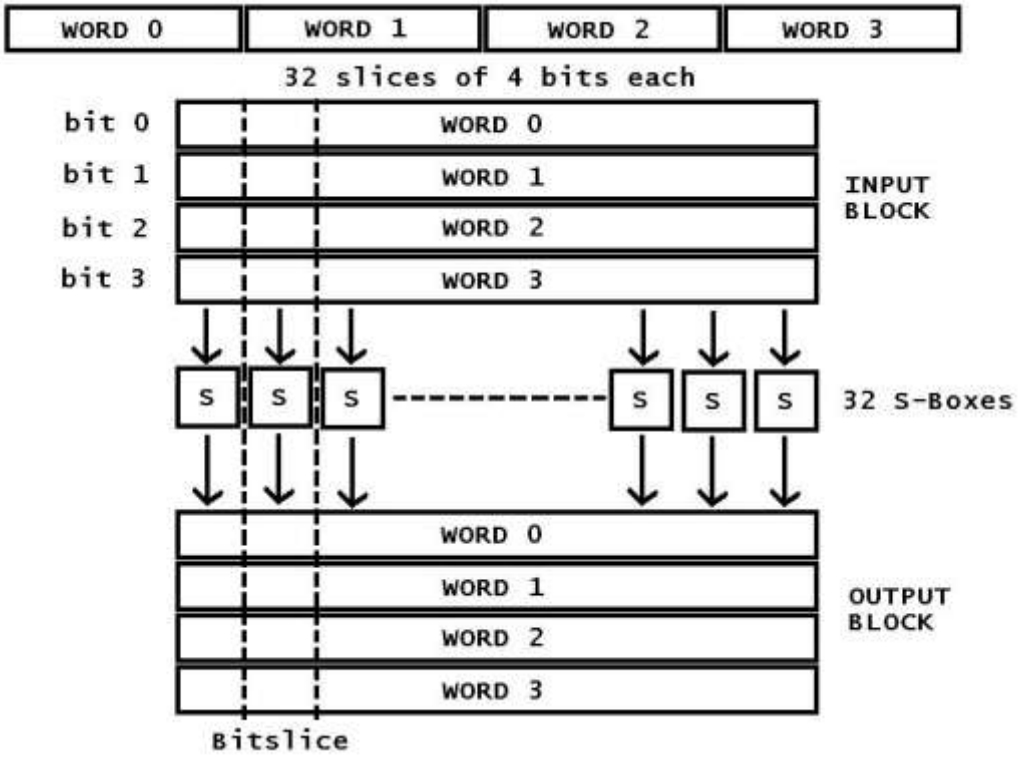


Figure 5: Serpent Algorithm Structure[13]

The Serpent algorithm has undergone a new modification that, according to [13], replaces the transformation of byte substitution (DES S-Box) in every round with 2 significant processes depending upon cyclic group substitution and logistic mapping. This will result in an increase in overall byte diffusion-confusion and an increase in the complexity of the alg'rithm's cryptanalysis, see Figure 6 [13]

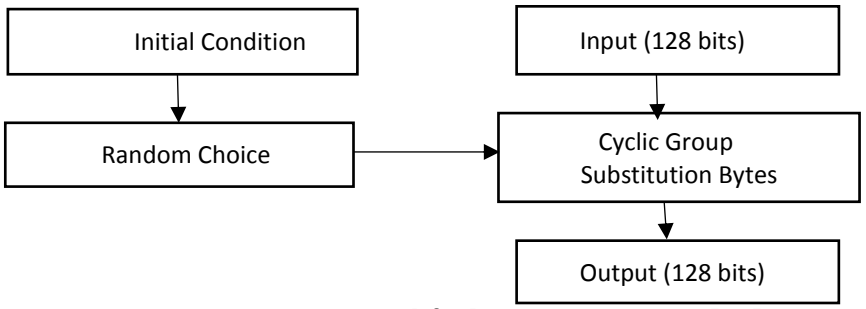


Figure 6: Modified Serpent Structure[13]

6- Analysis Tools

To assess the security of a particular system, a variety of analysis methods are utilized. The most well-known analysis tools are listed below: -

1- Entropy: This method involves gathering randomness for use in cryptography or other applications that call for random data from an operating system or application. This

randomness is frequently gathered from hardware sources, like HDD or fan noise variations, or from specially designed randomness generators. Security and performance might be negatively impacted by a lack of entropy [14].
2- Floating Frequency: The x-axis indicates distinct characters and the y-axis the number of bytes in the floating frequency of encrypted text, which means different characters every 64-byte block [15].
3- Histogram: In this method, continuous numerical ranges are used to group the data, and every range is represented graphically by vertical bar. The number range is shown on horizontal axis, and data amount in every one of the ranges is displayed on vertical axis (i.e., frequency). The ranges of numbers depend on the data being used [14].
4- Autocorrelation: In this method, the similarity degree between a given time series and lagged version of it over subsequent intervals of the time is mathematically represented. Though conceptually identical to correlation, autocorrelation utilizes the same time series twice: once in the original form, and once that is delayed by one time period or more [15].
5- Brute-Force Attack: This approach represents a cryptanalytic attack that relies on a method of trial-and-error to try to decrypt the cipher-text. The number of the r®ds (R), or R*Keylength, which represents a large number, determines the number of trials that cryptanalysts will require to crack the cyclic group sub bytes.

A brute-force attack entails the attacker submitting a number of the passphrases or passwords in hopes that one will be correctly deciphered eventually. All the potential passphrases and passwords are systematically checked by the attacker till the right one is discovered. An alternative is for an attacker to utilize a function of key derivation to try and guess the key, generated normally from the password, which is referred to as the exhaustive key search [167].

7- Proposed Cryptography Model (RCTS)

The short name of proposed model is (RCTS), which refers to the use of three efficient cryptography algorithms, the first one is RC5, second one is Twofish, and third one is Serpent algorithm. This research compared the efficiency of RCTS model with other algorithms by using the most important analysis tools like entropy, floating frequency, histogram, autocorrelation, and brute-force attack (key search space). In this research three cases were implemented as illustrated below: -

Case1: Single level Model 3441his

This case used only RC5 algorithm to encrypt every 64-bit block of plain text in normal state as illustrated previously in Figures (2-3). For example, suppose you have the following plain text and key:

(The science of cryptology, which mostly relies on arithmetic, analyzes the scientific elements of such methods (cryptanalysis and cryptography).

Key(256-bit)=
(0F0E0D0C0B0AA1B1C1D1E1F101020304050607080 99A9B8C8D7E7F1122334455). See Figure 7.

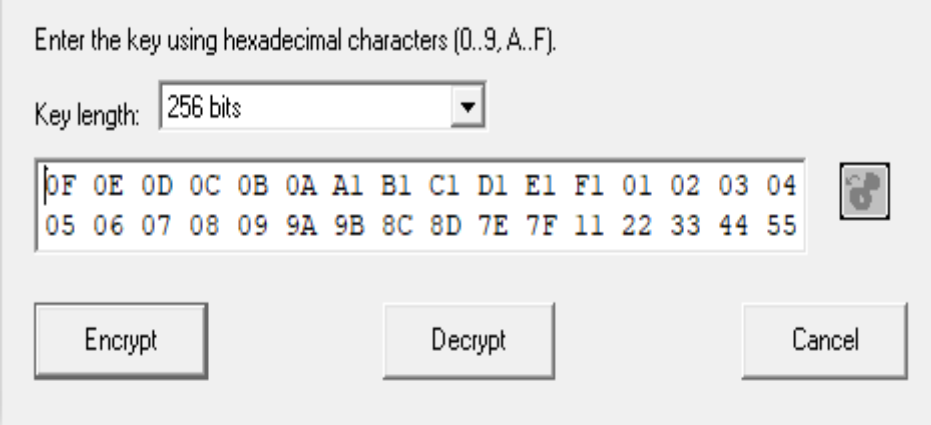


Figure 7: 256 key of RC5 Algorithm.

By applying RC5 algorithm, the following cipher text was obtained:
Cipher text:

```
0D 72 8B 2D C1 3C AB 53 0D 89 2D 21 FB D1 34 07 55 15 34 C2 0D 52 8D
F8 7F 3E FE B5 AA F5 13 69 7B C2 0D C6 95 AB 9D 56 84 F4 BF DC CE 15
8F B5 E2 74 80 72 C3 FE 3A B9 E5 C5 8F 98 06 46 C1 73 A0 22 21 F3 D4
9D FE 15 2F 8F 3E 67 DC 20 31 73 CB 88 BD 13 E8 00 32 C3 2C E8 7A A1
79 AA EF D8 CB 26 F7 04 CF 5D 3F 84 9C 97 A5 7C C4 BC 41 57 D1 59 0B
9C 43 CB A5 4F 7B E8 AC 31 ED B1 C1 53 A7 7E BA DE 7F 2E 2D 57 3E 8D
9C CB 27 F8 E4 F2 06 A7 A9 CB 3B 68 8B 59 D3 B0 E4 E9 C0 29 7E 2F
```

This is the simple and normal case of RC5 applied with 64-bit two times to generate 128-bit block. See Figure 8.

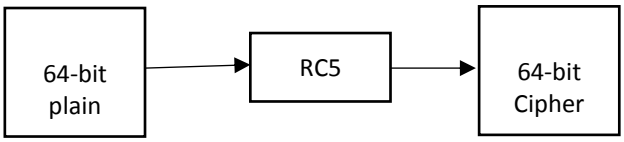


Figure 8: Case1- Single Level Model (RC5)

Case2: Bi-level Model (RC5 & Twofish)

This case used both RC5 & Twofish algorithms subsequently to encrypt the 128-bit plain. For example, suppose you have the same plain text used above with case1. Take the cipher text of case1 then encrypt it a second time by using Twofish algorithm with the following key:

Twofish key (256-bit)=
(0103050709020406080010 1A2B3C4D5E6FFFEEDDCCBBAAA1A2B1B2C1C2D1D2DD)
See Figure 9.

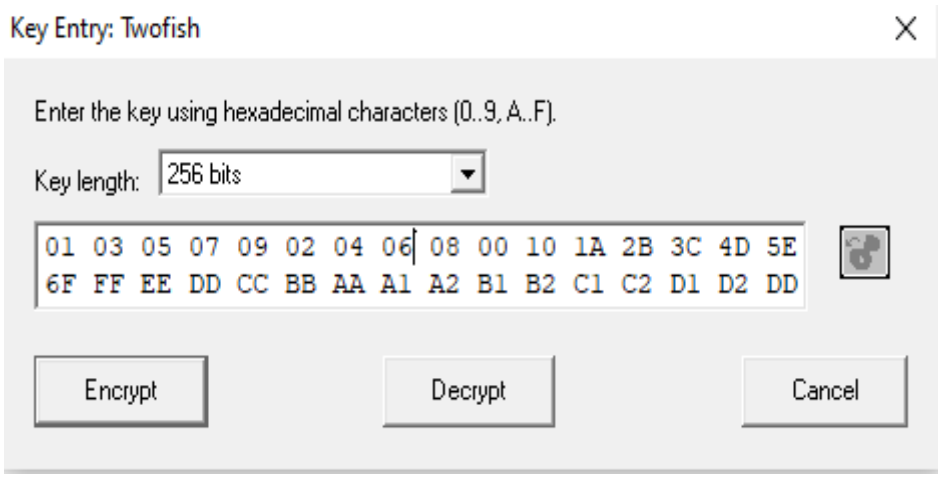


Figure 9: 256 key of Twofish Algori3443his

This case, when RC5 & Twofish algorithms are applied, the following cipher text was obtained:

```
C8 88 20 DE 69 BC 3C 18 A2 26 71 44 FC A6 EA DD 98 D1 6A 0E 3C AF B0
E3 25 86 FA A2 F3 95 81 AA D9 E2 52 A9 09 5C 5C AB DF 62 F8 DB 6E 6D
BB 70 A8 B1 20 21 86 F2 15 7A 7D 1D 00 27 1E 63 91 24 B0 33 CD 03 20
74 40 75 78 68 60 46 0C 9D 3F 1E F4 AE A0 84 0B 7E 53 81 9D 6D E8 68
65 99 78 52 8D 33 E2 21 F9 9D 2F 37 65 F8 43 55 5F 6F 14 3D D1 B5 4A
58 5F 0C B4 30 18 35 E7 E8 E6 9A BD 2C B2 58 7E 64 3B BC B5 01 6C 8C
02 20 B9 EA 7C 1E 13 25 FB A0 6C 84 45 C7 E9 22 AB 5C 6C E0 52 4A 6B
14 6F 06 F2 CE 91 B2 CA F5 E6 F3 87 33 FB DE
```

For more illustration of case 2, see Figure 10.

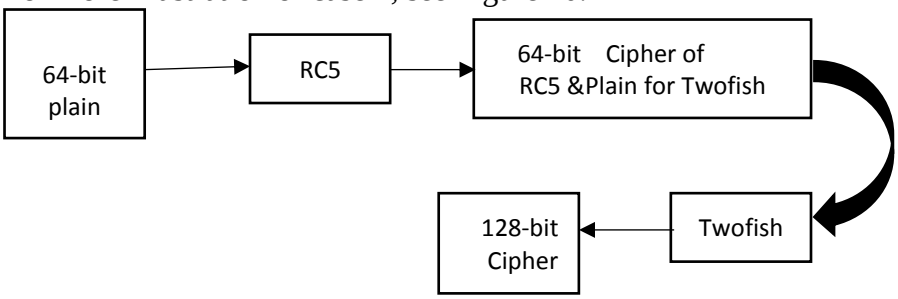


Figure 10: Case2- Bi-level Model (RC5 & Twofish)

Case3: Tri-tier Model(RC5 & Twofish & Modified Serpent)

In this case the proposed model used RC5, Twofish and modified Serpent algorithms sequentially to encrypt the 128-bit as illustrated in Figure 11.

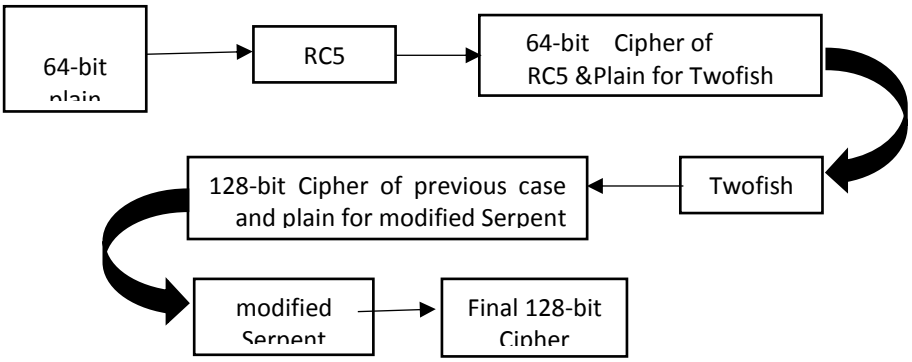


Figure 11: Case3: Tri-tier Model(RC5 & Twofish & Modified Serpent)

Also, this case used 256- bit key, as illustrated in Figure 12:-

(01AB5D4C8FFE98C1127563892CE2AD6F7859900256ED61AD902457FEE5592018)

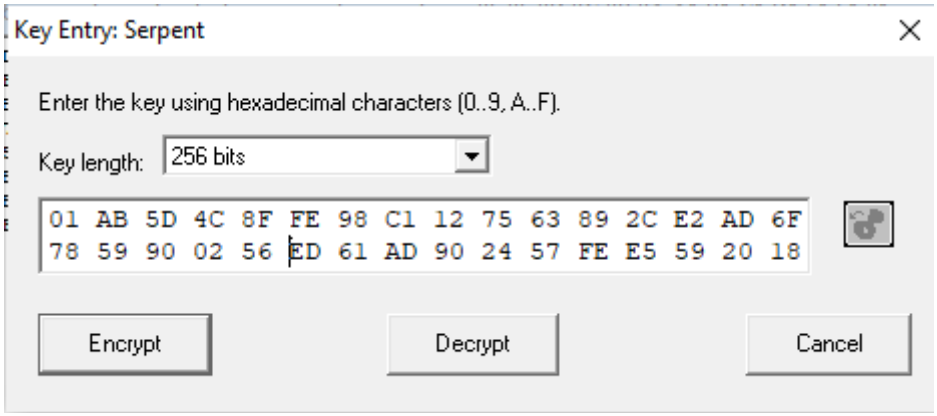


Figure 12: 256 key of modified Serpent Algorithm.

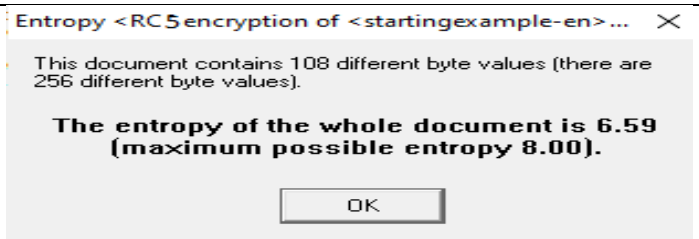
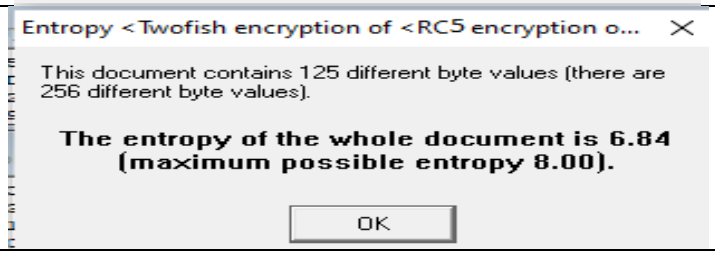
By applying RC5, Twofish, and modified Serpent algorithms, the following cipher text was obtained:

```
4B 11 CF 81 03 52 7D 1D 0F 02 A8 27 74 B6 3F E7 8B AD 22 88 29 01 C4
C9 BC 93 1F 71 D9 C3 B1 67 2B 27 15 2C DD 68 07 24 50 4C 57 1F 5A 46
A3 9E 47 FD 58 2B 6D 13 0B 6F E2 EB 7C A2 2F 78 91 E8 9D 54 95 F4 E0
52 C7 70 7D 15 98 80 9D B3 42 10 7B 22 EA 0F 7E 46 A2 F7 67 62 35 98
59 9D CC 1F 38 0F 3B 41 27 3D 38 81 19 3A E5 E4 A5 98 2D 48 67 D9 6A
6C CC AC 5C 5E E4 C2 1A 5C 82 DF 00 A7 12 B5 D2 EC EB CC 09 25 D1 3D
31 48 22 EC B2 B1 D5 D8 EF 49 B9 20 C9 67 FE 31 65 AB 82 8D A6 FD 8E
73 04 5C 83 62 04 8C 2B 97 19 55 66 5E 4D 61 B4 91 3F 0D 45 7D BF C9
CD 74 58 81 6A 84 5A 6E
```

8-Results Discussion

Table 1 shows the values of entropy of the three cases. It is noted that the value of entropy increases, and this indicates an increase in the complexity of the proposed model (case 3), that leads to more difficulty of cracking the cipher text for the attacker. As the value of entropy increases, it is much more difficult to obtain the plain text and the algorithm is stronger, as the attacker always looks for the lowest value of the entropy to make it easier to discover the key in the case of a brute-force attack.

Table 1: Entropy of three cases

Case No.	Analysis Tool (Entropy)
1	
2	

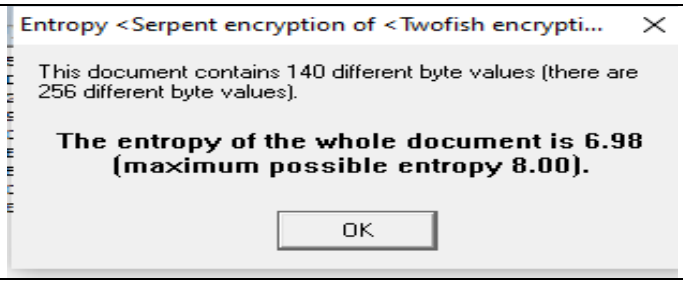
3	

Table 2 refers to another analysis tool, the floating frequency, where it presents the distribution of density. The difference of the model in the three cases more distribution of density with offset was obtained. Case3 was the best, as the character density in a specific window and the density is distributed.

Table 2: Floating Frequency of three cases

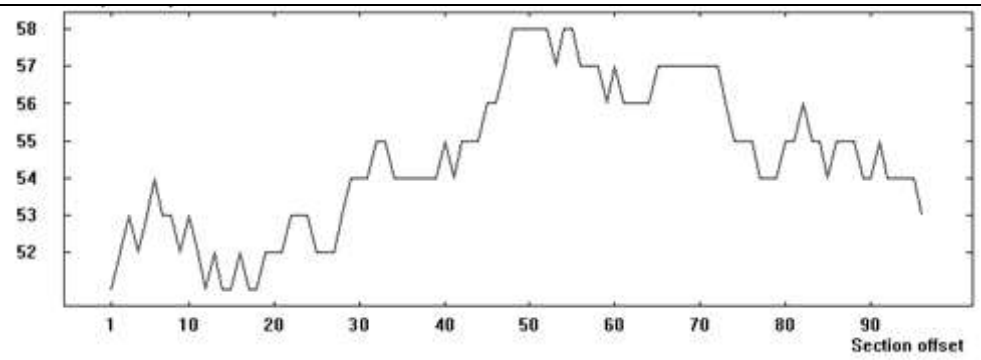
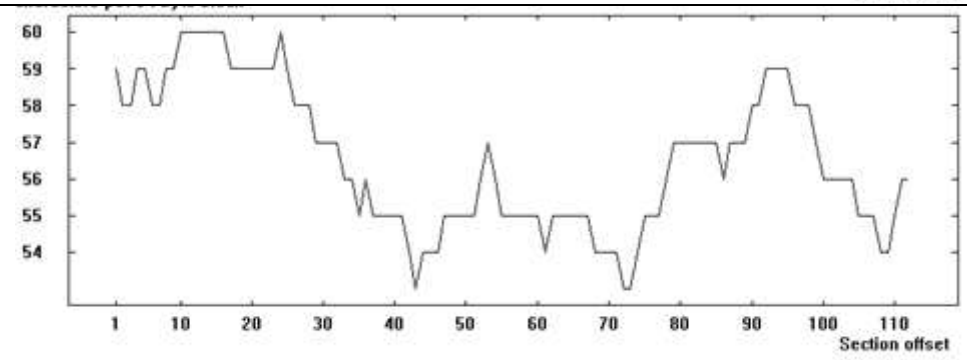
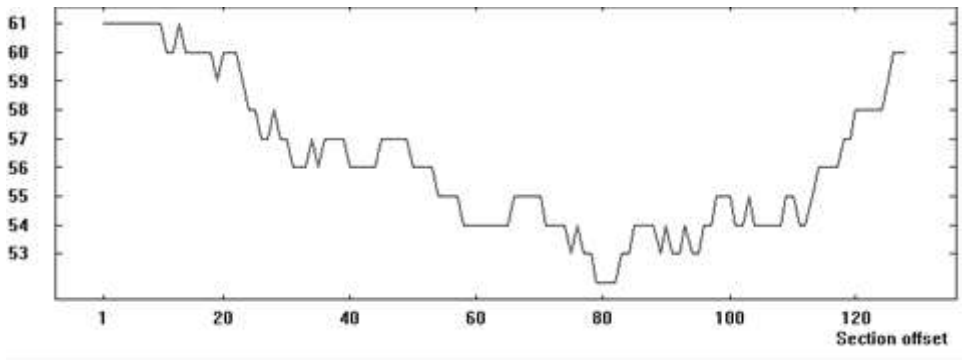
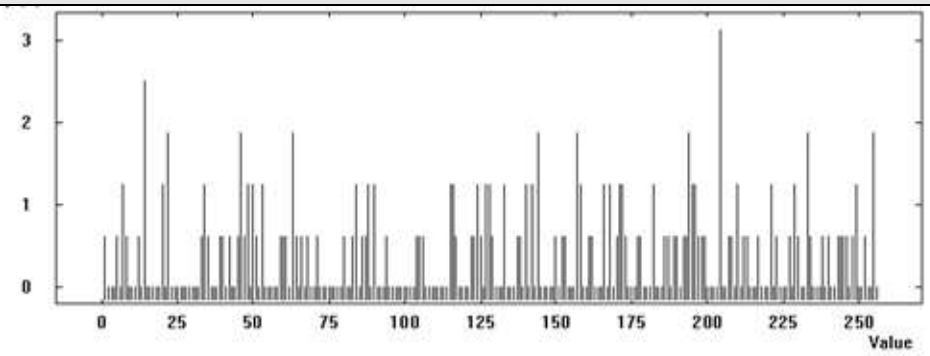
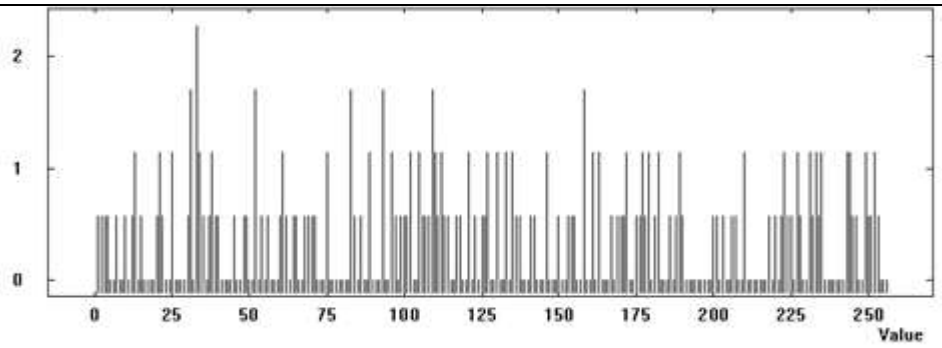
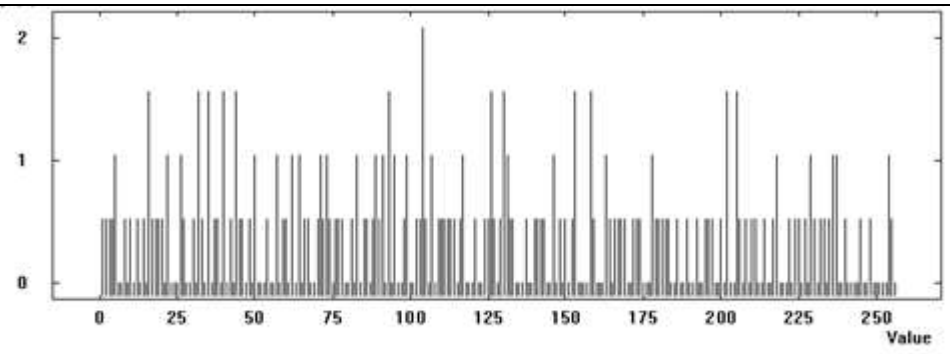
Case No.	Analysis Tool (Floating Frequency)
1	
2	
3	

Table 3 indicates, through the charts of the analysis tool called histogram, that case3 is the best as the diagram for the case1 (the y-axis), the value reaches 3, while the case 2 and case 3 the value of the y-axis is 2. That means that the number of times the character appears itself in the cipher text is reduced and this better where we have a diversity of the existing characters.

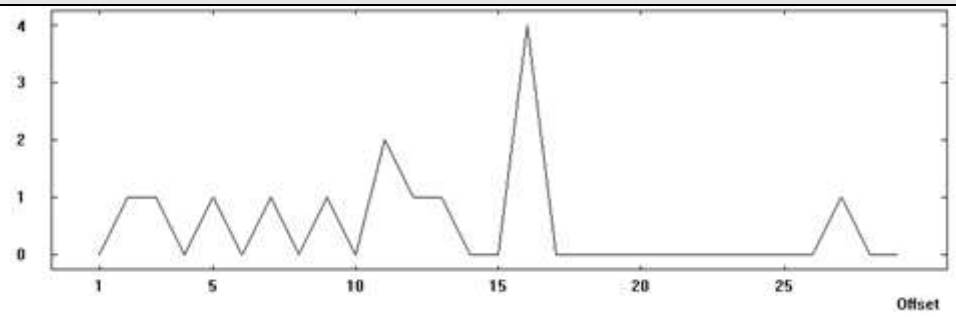
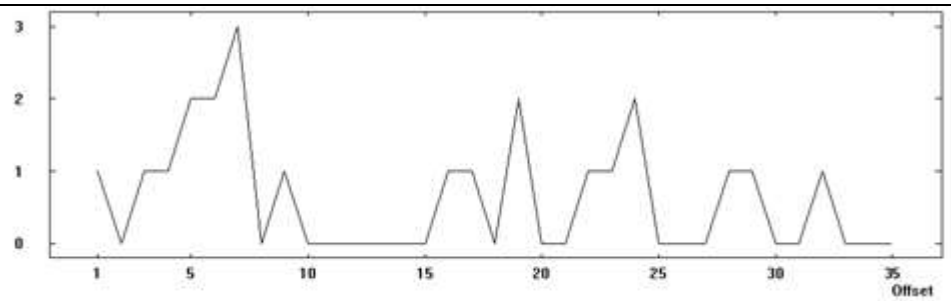
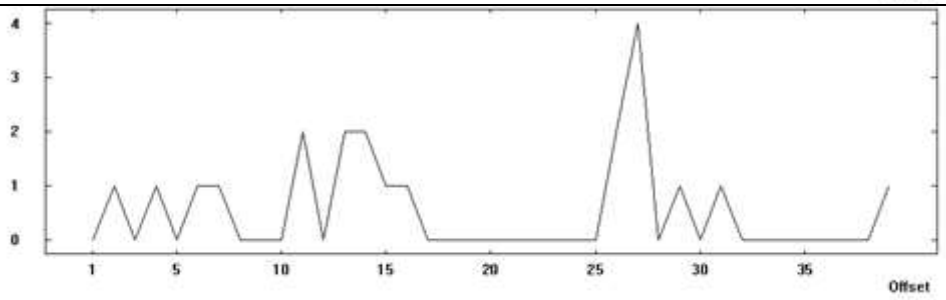
We also note that case3 is the best as it includes the appearance of more characters according to what is shown in the x-axis.

Table 3: Histogram of three cases

Case No.	Analysis Tool (Histogram)
1	
2	
3	

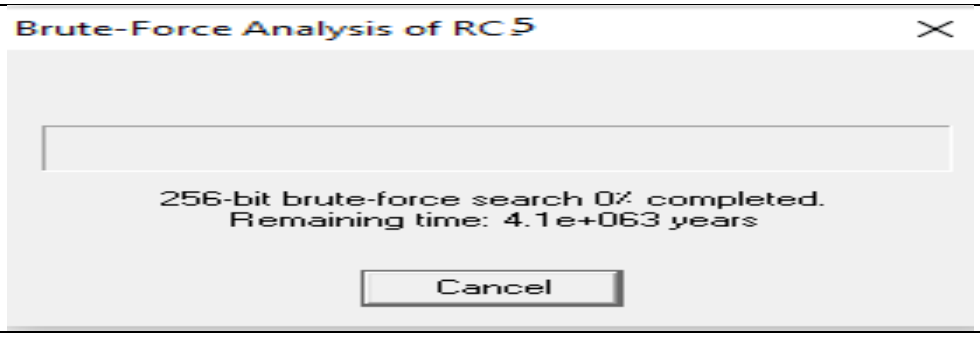
Autocorrelation is presented in Table 4, where we notice that the less autocorrelation, the better. This is what can be seen in case3, which represents the best case. The greater autocorrelation between the characters, leads to the attacker being able to crack the cipher text more easily, as attackers can deduce passages of plaintext, and gradually it is possible to access the key that was used for encryption and obtain the plaintext before encryption.

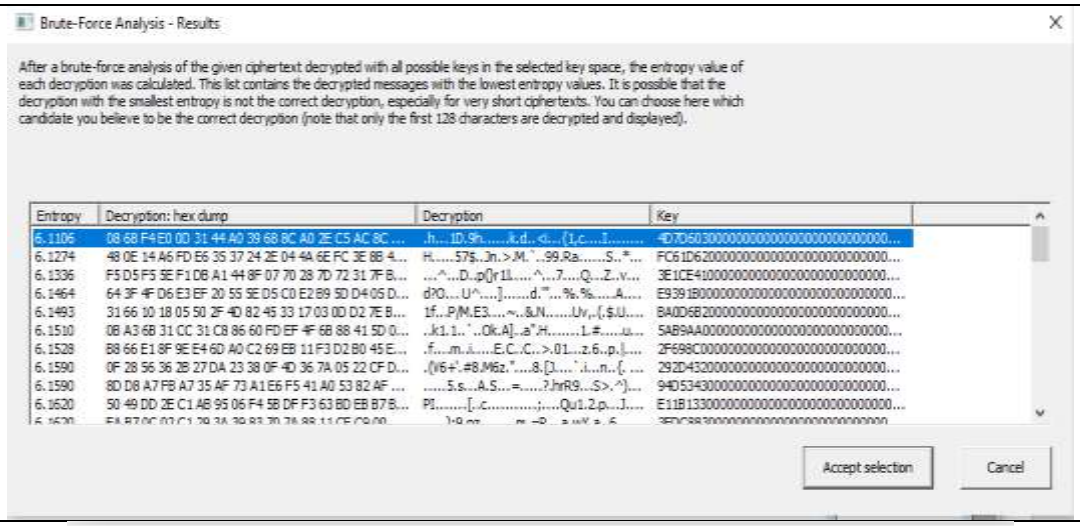
Table 4: Autocorrelation of three cases

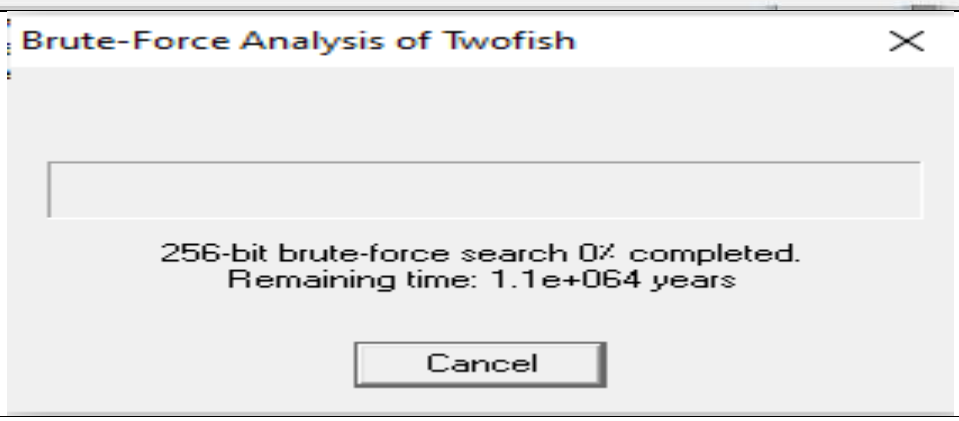
Case No.	Analysis Tool (Autocorrelation)
1	
2	
3	

As for the time it takes for the attacker to execute the brute-force attack, in case 3 it takes much more time to get the key needed to obtain the original message (see Table 5). The complexity also increases with the increase in levels numbers, where for each level the key of the specific algorithm used with long 256 bits. The number of probabilities for the key with the time required to discover it as shown in Table 6.

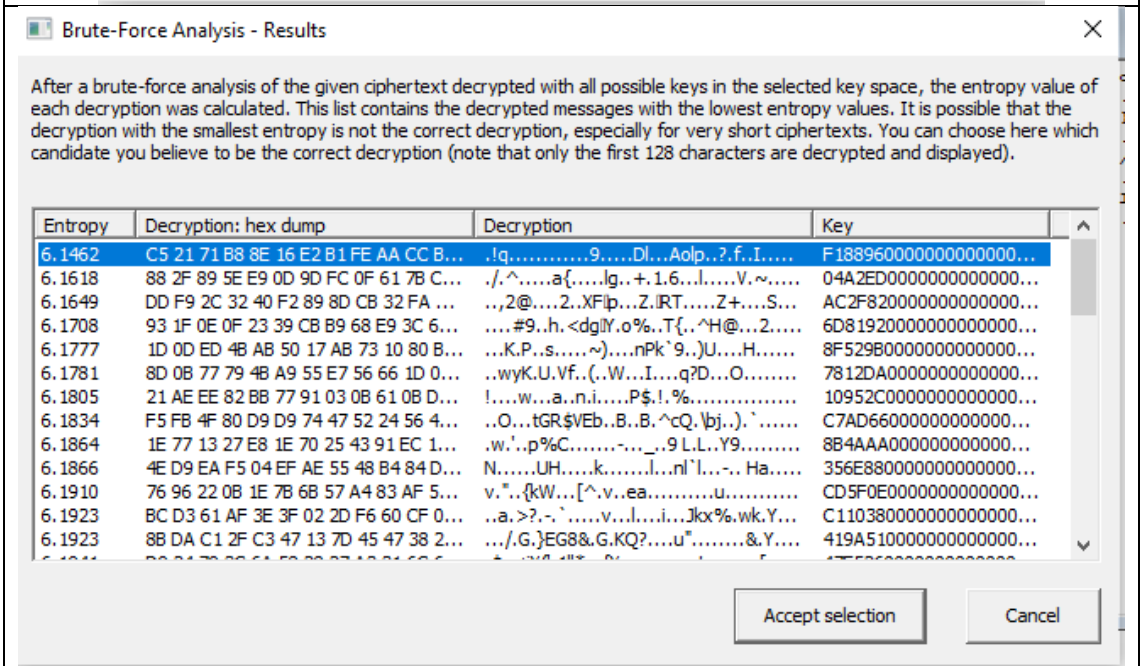
Table 5: Time of Brute-force Attack of three cases

Case No.	
1	

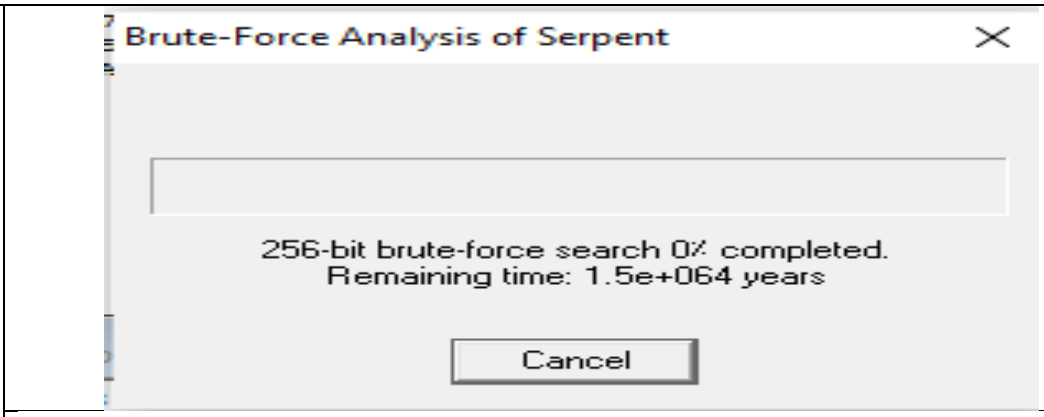

Brute-Force Analysis - Results
After a brute-force analysis of the given ciphertext decrypted with all possible keys in the selected key space, the entropy value of each decryption was calculated. This list contains the decrypted messages with the lowest entropy values. It is possible that the decryption with the smallest entropy is not the correct decryption, especially for very short ciphertexts. You can choose here which candidate you believe to be the correct decryption (note that only the first 128 characters are decrypted and displayed).
Entropy
Decryption: hex dump
Decryption
Key
Accept selection
Cancel


Brute-Force Analysis of Twofish
256-bit brute-force search 0% completed.
Remaining time: 1.1e+064 years
Cancel

*2


Brute-Force Analysis - Results
After a brute-force analysis of the given ciphertext decrypted with all possible keys in the selected key space, the entropy value of each decryption was calculated. This list contains the decrypted messages with the lowest entropy values. It is possible that the decryption with the smallest entropy is not the correct decryption, especially for very short ciphertexts. You can choose here which candidate you believe to be the correct decryption (note that only the first 128 characters are decrypted and displayed).
Entropy
Decryption: hex dump
Decryption
Key
6.1462 C5 21 71 B8 8E 16 E2 B1 FE AA CC B... .!q.....9.....Dl...Aolp..?.f..I..... F188960000000000000...
6.1618 88 2F 89 5E E9 0D 9D FC 0F 61 7B C... ./.^.....a{.....lg..+.1.6...l.....V.~..... 04A2ED00000000000000...
6.1649 DD F9 2C 32 40 F2 89 8D CB 32 FA ... ..,2@....2..XFlp...Z.lRT.....Z+....S... AC2F820000000000000...
6.1708 93 1F 0E 0F 23 39 CB B9 68 E9 3C 6... ....#9..h.<dg!Y.o%..T{..^H@...2..... 6D81920000000000000...
6.1777 1D 0D ED 4B AB 50 17 AB 73 10 80 B... ...K.P..s.....~)....nPk`9..)U....H..... 8F529B0000000000000...
6.1781 8D 0B 77 79 4B A9 55 E7 56 66 1D 0... ..wyK.U.Vf..(..W...I....q?D...O..... 7812DA0000000000000...
6.1805 21 AE EE 82 BB 77 91 03 0B 61 0B D... !....w...a..n.i.....P$.!.%..... 10952C0000000000000...
6.1834 F5 FB 4F 80 D9 D9 74 47 52 24 56 4... ..O...tGR$VEb..B..B.^cQ.\bj..).`..... C7AD660000000000000...
6.1864 1E 77 13 27 E8 1E 70 25 43 91 EC 1... .w.'..p%C.....-..._..9 L.L..Y9..... 8B4AAA000000000000...
6.1866 4E D9 EA F5 04 EF AE 55 48 B4 84 D... N.....UH.....k.....l...nl`l...-.. Ha..... 356E880000000000000...
6.1910 76 96 22 0B 1E 7B 6B 57 A4 83 AF 5... v."..{kW...[^.v..ea.....u..... CD5F0E0000000000000...
6.1923 BC D3 61 AF 3E 3F 02 2D F6 60 CF 0... ..a.>?.-.`.....v...l....i...Jkx%.wk.Y... C110380000000000000...
6.1923 8B DA C1 2F C3 47 13 7D 45 47 38 2... .../.G.}EG8&.G.KQ?....u".....&.Y..... 419A510000000000000...
Accept selection
Cancel

3



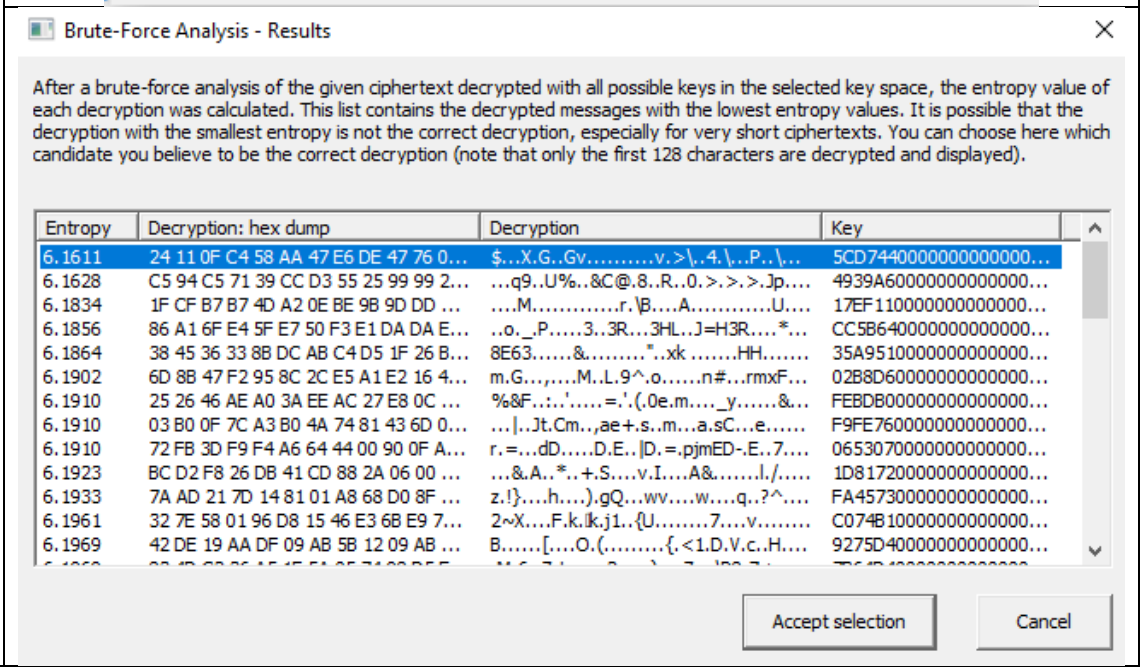


Table 6: Brute-force Attack According key length and Required Time

Case no.	Key Search Space	Brute-force Attack Time
1	2^{256}	4.1e+063
2	$2^{256} * 2^{256}$	1.1e+064
3	$2^{256} * 2^{256} * 2^{256}$	1.5e+064

The 256-bit key has 2^{256} possible combination values, as was stated previously. Thus, whenever the exponent is raised, the number of potential combinations would considerably increase. 2^{256} is 2x2, x2, x2……256 times. The optimal way of cracking an encryption key is using the 'brute-force attack,' which is merely trial and error in the simple terms. Thus, in the case where the length of the key is 256-bits, there would be 2^{256} possible combination values, and the hacker would have to try the majority of the 2^{256} potential combination values prior to the extraction of the key. Potentially, it will not require trying all those combinations for guessing the key –often it is approximately 50% –however, the time that it would take to do that would be more than any human lifespan.

9 Conclusions

A good encryption model should have a strong resilience against attacks that attempt to break the system, such as brute force attacks. Resistance against attacks is a good measure of the performance of a cryptography system. key space should be big enough to inhabit brute

attack. In this research, the proposed encryption model RCTS presented secure analysis compared to case-1 and case-2, Therefor the proposed model proved its efficiency and, provided reasonable security against cryptanalysis by using different analysis tools like entropy, floating frequency, histogram, autocorrelation, and brute-force attack. In addition, the increase the complexity of the encryption model that leads to attackers requiring increased time to crack the cipher text. The proposed model increased the search space of key by using three keys in case-3 ($2^{256} * 2^{256} * 2^{256}$).

Refrences

[1] M.Mayes Hoobi, " Keystroke Dynamics Authentication based on Naïve Bayes Classifier ", *Iraqi Journal of Science* , Vol 56, No.2A, pp:1176-1184, 2015.

[2] M.Mays Hoobi," Improved Structure of Data Encryption Standard Algorithm", *Journal of Southwest Jiaotong University*, Vol. 55 No. 5 Oct. 2020.

[3] H. Halah and M.Mayes," Improved Rijndael Algorithm by Encryption S-Box Using NTRU Algorithm", *Iraqi Journal of Science*, Vol 56, No.4A, pp: 2982-2993,2015.

[4] P.PATIL and P. NARAYANKAR and D.G.NARAYAN and S.M. MEENA, " A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish ", Procedia Computer Science, pp. 617-624, 2016.

[5] M .HOOBI, "Strong Triple Data Encryption Standard Algorithm Using Nth Degree Truncated Polynomial Ring Uni", *Iraqi Journal of Science*, 58 (3C), pp. 1760-1771, 2017.

[6] M.Mayes Hoobi, "Efficient Hybrid Cryptography Algorithm", *Journal of Southwest Jiaotong University*, Vol 55, No 3, 2020.

[7] M. HOOBI and S.S .SULAIMAN ,"Enhanced Multistage RSA Encryption Model", Proceedings of the 2nd International Scientific Conference of AlAyen University, July 2020.

[8] G N. Krishnamurthy and Dr. V Ramaswamy, "Performance Analysis of Blowfish and its Modified Version using Encryption quality, Key sensitivity, Histogram and Correlation coefficient analysis of Information", *International Journal of Recent Trends in Engineering*, Vol. 1, No. 2, May 2009.

[9] A. T Hashim,and R. F. Nathim, and G. Saeed Mahdi, "Modification of RC5 Algorithm for Image Encryption,*", IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL SYSTEMS ENGINEERING*, vol. 14, no. 2, pp. 62-71, 2014

[10] D. Gulsezim, "Two factor authentication using twofish encryption and visual cryptography algorithms for secure data communication," Sixth Int. Conf. on Internet of Things: Systems, Management and Security (IOTSMS*)*, Granada, Spain, pp. 405–411, 2019.

[11] W. Sun and G. C. Zhang and X. R. Zhang and X. Zhang and N. N. Ge, "Fine-grained vehicle type classification using lightweight convolutional neural network with feature optimization and joint learning strategy" , *Multimedia Tools and Applications*, vol. 80, pp. 30803–30816, 2021.

[12] M.Hassan and A. Mahmoud, "New Encryption Technique Using the Meaning of Location Algorithm" , Application of Information and Comm. Tech. Conference, pp. 206-210, 9 Oct. 2015.

[13] M. Hassan and E. Takieldeen and A.Mahmoud Shawky, "A Modified Serpent Based Algorithm for Image Encryption", 35th NATIONAL RADIO SCIENCE CONFERENCE , March 27 - 29, 2018.

[14] A. Sciacovelli and V.Vittorio and S.Enrico, "Entropy generation analysis as a design tool—A review", *Renewable and Sustainable Energy R-eviews,*pp 1167-1181,2015,.

[15] B. Brumen and T. Makari, "Resilience of students' passwords against attacks," Information and Communication Technology, Electronics and Microelectronics (MIPRO) 40th International Convention, pp. 1491–1495,2017.

[16] L. Bošnjak and B. Brumen, "What do students do with their assigned default passwords?," *Information and Communication Technology, Electronics and Microelectronics (MIPRO) 39th International Convention*, pp. 1430–1435,2016.

[17] Harba.H, Abdulmunem.I, Hussein.S, "Improving security of the crypto-stego approach using time sequence dictionary and spacing modification techniques", *Iraqi Journal of Science*, Vol.62,issue-5, pp. 1721–1733, 2021.