Article

JOURNAL OF UNIVERSITY OF BABYLON

For Pure and Applied Sciences (JUBPAS)

Vol.32; No.2.| 2024

Improvement the International Data Encryption Algorithm(IDEA)based on Chaos Theory

Nadia Abed AL- Khaleak Gabar[1*], Mohammed Abdullah Naser [2]

1College of Science for Women, University of Babylon, nadia.almosawi.gsci147@student.uobabylon.edu.iq, Babylon, , Iraq.

2College of Science for Women, University of Babylon, wsci.mohammed.abud@uobabylon.edu.iq , Babylon, Iraq.

***Corresponding author email:** nadia.almosawi.gsci147@student.uobabylon.edu.iq; mobile: 07829928926

تحسين خوارزمية تشفير البيانات الدولية بالاعتماد على نظرية الفوضى

نادية عبد الخالق جبار*[1]، محمد عبدالله ناصر[2]

1 كلية العلوم للبنات، جامعة بابل، nadia.almosawi.gsci147@student.uobabylon.e

Accepted: 1/4/2024 **Published:** 30/6/2024

ABSTRACT

Background:

The (IDEA), which represents International Data Encryption Algorithm is a widely used cipher algorithm that has raised concerns due to the discovery of numerous weak keys, as highlighted in previous research. These weak keys, specifically those containing consecutive sequences of single digits, have been found to impede the algorithm's evolution and result in a sluggish avalanche effect. To address these vulnerabilities, this research aims to develop an enhanced and secure encryption algorithm by incorporating Chaos Theory principles into IDEA.

Materials and methods:

The primary objective is to address the weaknesses associated with IDEA's key generation process by leveraging Chaos Theory to generate strong, highly random keys that replace the algorithm's weak keys t. The study also aims to assess the security and cryptographic strength of the enhanced IDEA algorithm through evaluations and comparisons with the original algorithm.

Results:

The results showed that the proposed key passed 11 tests out of the 15 total tests, while the Traditional key of IDEA passed only 7. This indicates that the proposed method is superior by 4 tests over the Traditional method of generating keys. Also, cipher text 1 with the proposed key passed 10 tests out of the 15 total tests, while with the Traditional key passed only 8 .

Conclusion:

This indicates the superiority of the proposed method of IDEA in encryption over the traditional method of IDEA.

Key words:

Traditional algorithm, Suggested algorithm, Secure Cipher text, Chaotic system, NIST.

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

INTRODUCTION

Data is the real core of any contemporary digital business. it generates services and products from user experiences and visions. It is crucial to think about both digital and physical safety at the same time since securing the areas where we keep our belongings and data stored is just as vital. The three main goals of data security are availability, integrity, and confidentiality [1].

Encryption is one of the major extensively utilized well known tool for achieving data security [2]. It is the technique and science of cryptography that includes numerous security features like digital signatures and identification [3]. Additionally, the mathematical process of converting a cipher to original text and reversely is how the encryption algorithm is specifically described [4]. In a cipher system, there is a mathematical process involved in encrypting and decrypting messages. For the majority of individuals, using cryptography to keep communication hidden comes first. It has been widely known and recognized that utilizing cryptography is essential for protecting private communication. However, this is only a small portion of how cryptography is used today [5]. A block cipher called the International Data Encryption Algorithm (IDEA) was created in 1991 by James Massey, Xueija Lai, and ETH-Zürich. IDEA was once known as IPES (Improved PES), and it represents a slight improvement of Proposed Encryption Standard (PES) was an early encryption. In the initial iterations of the cryptosystem excellent privacy, IDEA functioned as the symmetric cipher. IDEA was tasked with creating a powerful encryption algorithm to take the place of the DES method created in the USA in the 1970s. It is particularly intriguing because it completely ignores the use of S-boxes and lookup tables. Phil Zimmermann built the ubiquitous PGP file and email encryption program with maximum security. They chose IDEA as their initial option for data encryption because of its excellent reputation and tried-and-true design [6]. According to Daemon study [7], a considerable number several weak keys for the IDEA block cipher system have been found. It is shown that a considerable modification of the IDEA key scheduling may address the weak key problem. In 1963, Edward Lorenz used chaos for the first time amongst the most important hypotheses for producing an predictable sequence. The secrecy of an encryption system should reside in the key rather than the encryption or decryption algorithm. While developing a powerful cryptosystem, one of the most intriguing issues for academics to investigate is chaos [8]. Due to their benefits, including pseudo-

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

randomness, unpredictability, ergodicity, lack of periodicity, and great sensitivity to initial circumstances and control settings, chaotic maps have captured the curiosity of numerous researchers in lately [9]. Because they are unpredictable and deterministic, these characteristics are adequate as well as advantageous for depending on them to produce cypher system keys. This is due to the primary foundation of cipher system security is the incapacity to predict and possess the keys [10]. The objective of this research is to improve and secure IDEA by integrating the ideas of Chaos Theory. Using Chaos Theory to produce strong, extremely random keys to replace the algorithm weak keys.

MATERIALS AND METHODS

Compare more encryption algorithms

The General Structure of the Suggested System

The system's overall framework shows the mechanism of the encryption process for the encryption system using the IDEA It compares two methods: the traditional method and the proposed method. The traditional method uses a straightforward encryption process by IDEA, taking plain text and converting it into encrypted data using traditionally of IDEA. The traditional key is broken down into 52 subkeys, where the main key is divided into smaller parts for the encryption process. The proposed method includes additional elements not present in the traditional, by using Chaos theory (Cat map and Henon map) such as xCat, yCat, xHenon, and yHenon, which refer to variables or parameters in a more complex encryption algorithm. The "Generate Key" function implies that the proposed method involves dynamic random key generation, making it more secure. this function generates a random 832-bit key and enhances security by making it more difficult to predict the encryption key.

The proposed method is an advancement over the traditional by introducing an additional layer on the generation of key (a type of chaotic mathematical function that might be used to increase the randomness of the encryption). The design and implementation of each of these two methods will be explained in detail. Finally, (the traditional key of the algorithm, its proposed key, the ciphertext of the traditional algorithm, and the ciphertext of the algorithm after modification) are assessed a series of 15 NIST tests to prove the security and confidentiality of the traditional algorithm, suggested algorithm, and their relevant keys. The overall design of the suggested system is illustrated in Figure 1.1.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

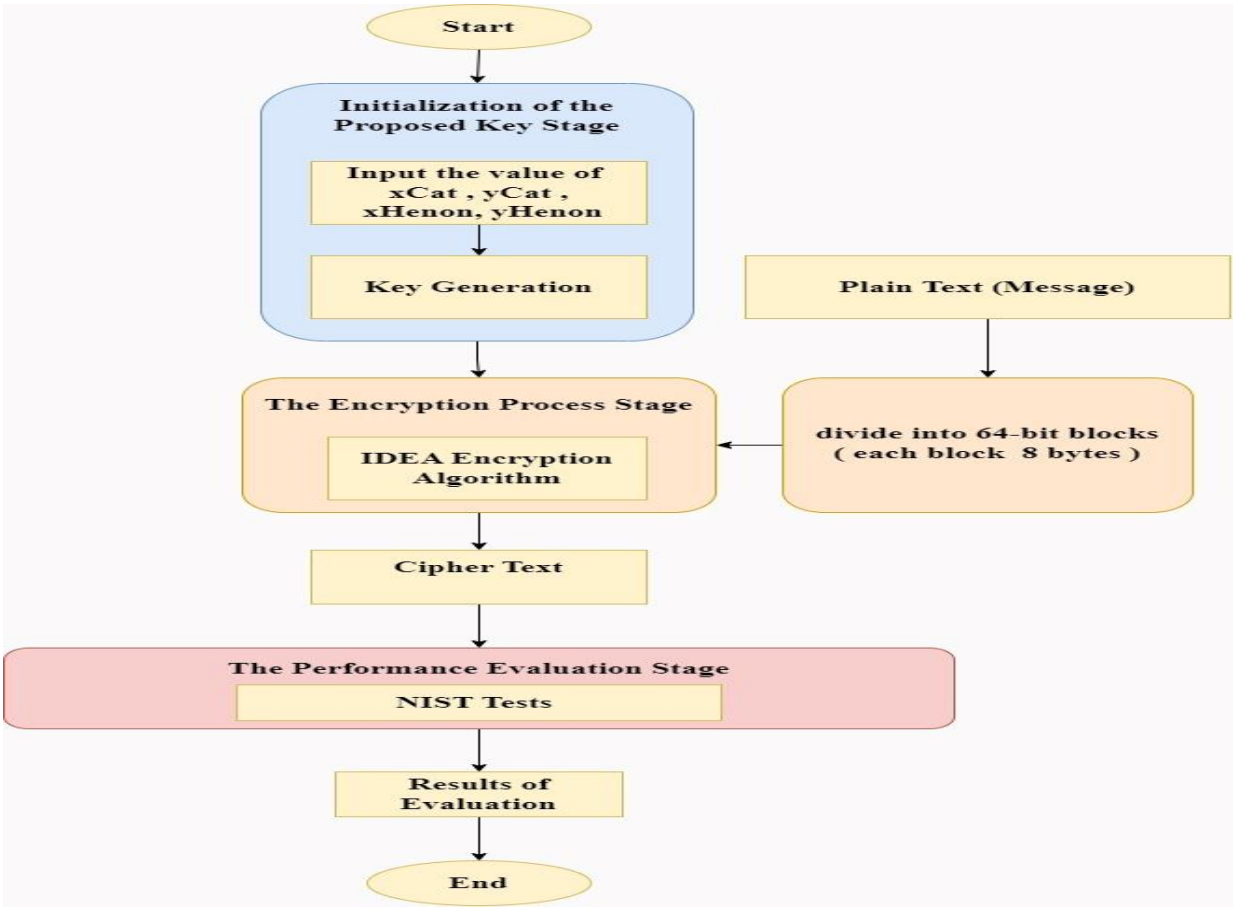

Figure1.1 General Block Diagram of the Proposed System

The Proposed Key Generation Stage

we will discuss all the details of the proposed key generation based on chaotic systems, as follows:

Setting Parameter Values

Creating chaotic behavior on chaotic maps, for instance, Henon Map and Cat Map, requires setting parameter values[11]. You may experiment with different values of (x_i, y_i, x_m, y_m) to get chaotic behavior. The chaotic behavior of the map will change if the values of (x_i, y_i, x_m, y_m) are changed, becoming more or less random. The beginning conditions and parameter settings have a significant impact on the chaotic behavior. To get the necessary chaotic features, you might

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

need to run tests and examine the behavior of these maps because little adjustments can have a big impact on the results.

Secure Chaos Keys Generation (SCKG)

Because chaotic systems' output numbers have unpredictability properties, many researchers propose embedding the chaotic system into their work[12]. For many researches over the last years, the chaos keys have been used extensively for encryption operations.

The 2-D Chaos was proposed and designed because the IDEA algorithm needs to use secure and strong keys to enhance its security. The (SCKG) technique elucidates the process of generating a hybrid method that combines two maps from a chaotic system(2D Cat map and 2D Henon map) to generate random chaos keys, as outlined in Equation 1.1, that illustrated below sequentially which generate an extremely random set of numbers that combination with IDEA algorithm to enhance its performance and offered a significant degree of chaotic encryption.

$$
\begin{aligned}
x_{m+1} &= (2x_m + y_m) mod\ 1. \\
y_{m+1} &= (x_m + y_m) mod\ 1. \\
x_{i+1} &= 1 - a x_i^2 + y_i,. \\
y_{i+1} &= b x_i.
\end{aligned}
\qquad (1.1)
$$

Where (x_{m+1}, y_{m+1}) and (x_{i+1}, y_{i+1}) denote the new state of the two-dimensional coordinates (x_m, y_m) and (x_i, y_i) respectively, representing the current state. The parameters (b=0.3) and (a=1.4) represent two variables utilized in the equations of the Henon chaotic Map.

The proposed method as shown in Figure 1.2 applies mathematical operations such as the add and multiplication to integrate the outcomes of the two maps. The initial values specify the security and randomness for this method.

Article
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Vol.32; No.2.| 2024

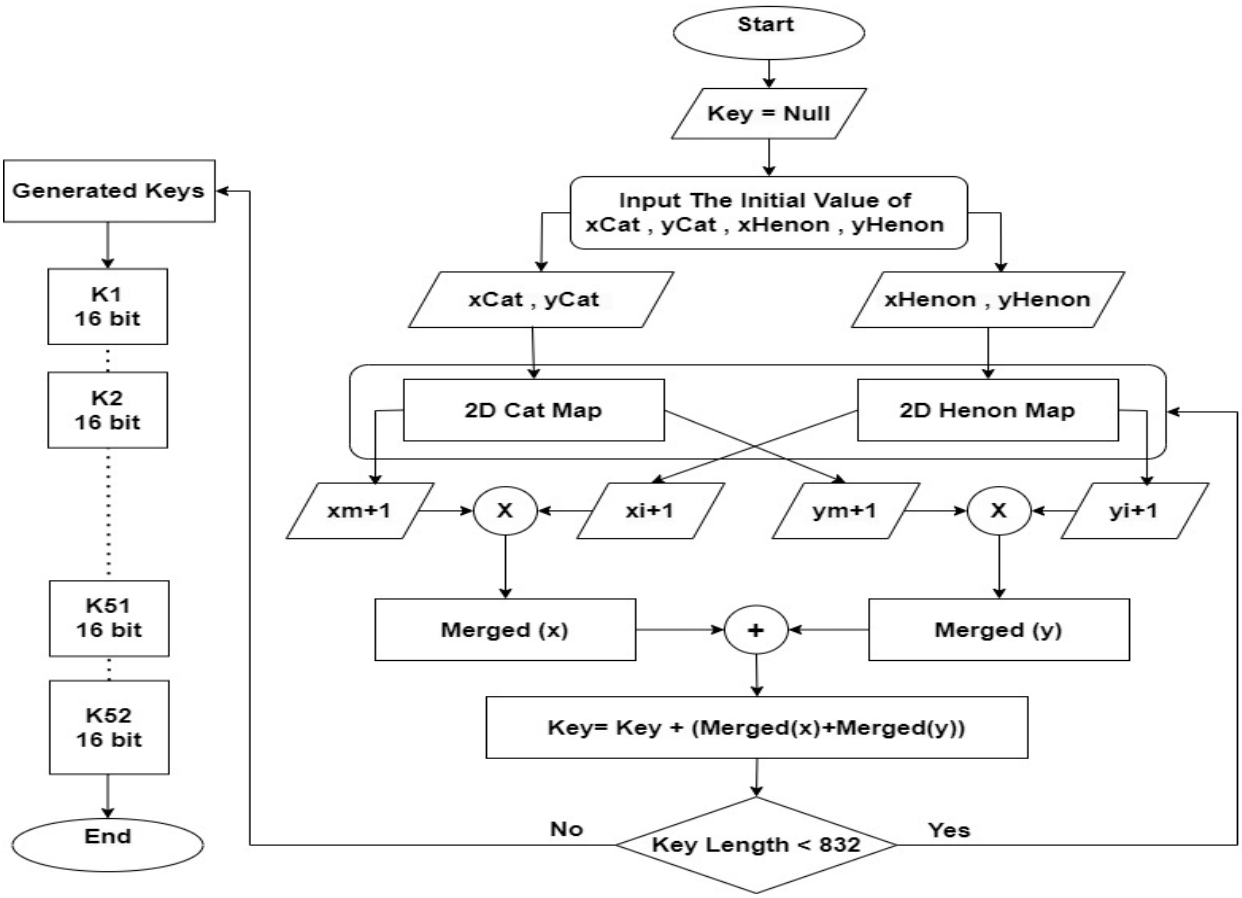

Figure 1.2. Block Diagram of the Proposed Keys Generator (SCKG)

The generated chaos keys (K1...K52) are used in the IDEA algorithm.

Algorithm 1.1 displays the Chaos key generation.

Algorithm 1.1. The Secure Chaos Keys Generation (SCKG)

Input: parameters and Initial variables.

Output: Chaotic Keys: (K1, K2, …, K52).

Begin

Step1: Input the initial values of Henon map $(x_i,\ y_i)$ and cat map $(x_m,\ y_m)$, In addition to values of α, $\beta$where α=1.4 and β=0.3.

Step2: utilize the equation (1.1) to calculate the values of (x_{i+1}, y_{i+1}) and (x_{m+1}, y_{+1}).

Step3: Apply Multiplication$(x_{i+1},\ x_{m+1})$ to obtain Merged(X) and Multiplication (y_{i+1}, y_{m+1}) to obtain Merged (Y).

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Step4: Perform Add Process between the Merged (X) and Merged (Y) to obtain sequence with high randomization and add this to Key.

Step 5: If Length of Key less than 832 bit, return to Step 2.Else Generated Key process is finished.

End.

The algorithm then generates 52 subkeys, each of 16 characters, from the main key. These keys can be useful in secure communications, where unpredictability and resistance to pattern detection are crucial.

Plaintext Initialization

The 64-bit plaintext blocks that the (IDEA) operates on[13]. Each 64-bit block that makes up the input plaintext is encrypted separately. There are four sixteen-bit subblocks within this 64-bit input plaintext block. These sunblock's of sixteen bits are subjected to eight similar changes, called rounds, and then a half round modification of the output. The ciphertext block has the same size as the 16-bit plaintext block. Block ciphers work in round blocks, applying a portion of the encryption key—referred to as the round key—to each round before performing additional mathematical operations. It generates the ciphertext for that block after a specific amount of rounds.

If the plaintext input to the IDEA is smaller than 64 bits, it cannot directly fill the required block size of the algorithm, which is designed to operate on 64-bit blocks. In such a case, the plaintext must be padded to reach the necessary block size[14]. When using zero padding, zeros are included in the end of the plaintext until it exceeds the necessary 64-bit length. When the plain text input to IDEA is larger than 64 bits, the 64 bits are cut off one by one. If there is a remainder, it is also Compensated with zeros until the last 64 bits. **Figure 1.3** shows the Plaintext Initialization process.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

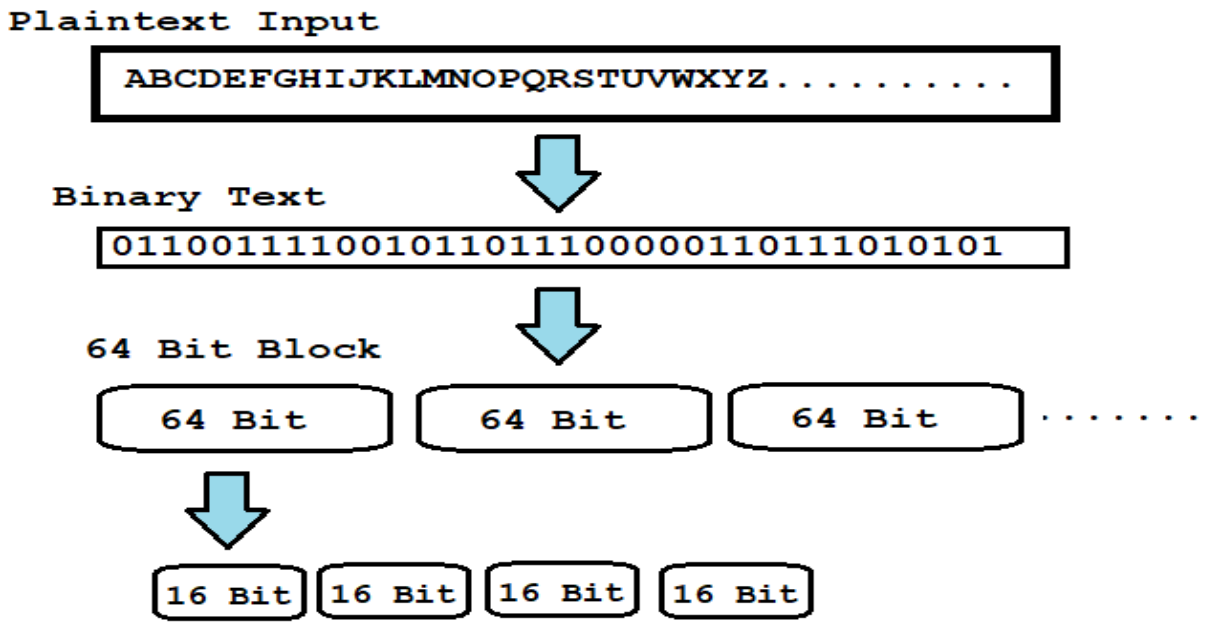

Figure 1.3. Plaintext Initialization process

The Encryption Process Stage

In this stage, the encryption process will be clarified using the IDEA algorithm with its traditional key, in addition to clarifying the encryption process using the proposed key.

The Encryption Process with Traditional Key

In the Encryption Process with the traditional Key, the IDEA algorithm is implemented without any change in its original structure. This process takes place through several steps described below:\

Initialization and Input plaintext:

Retrieves plaintext input from a UI element and converts it into a byte array. The byte array has a length that is a multiple of 8 (it works with 64-bit blocks, with each block being 8 bytes).

Key Processing:

Extracts a string of key values (kText). It checks if the key length is 832 bits (104 bytes). Splits this key string into 52 parts, each representing a 16-bit value, and stores them in an array (kValues).

Block Processing:

Processes each 64-bit block of the input text. This involves splitting the block into 4 parts (pValues), each 16 bits (2 bytes) in size. For each part, a series of transformations is applied

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

using subsets of kValues. These transformations involve bitwise operations and permutations typical in cryptographic algorithms.

Transformation Rounds:

For each part of the block, it undergoes 8 rounds of transformations, each time using a different set of 6 values from kValues. After each round, it updates the UI element with the current state of the part in binary form.

Final Transformation:

After the 8 rounds, a final half-round transformation is applied to each part using the last 4 values from kValues. The final state of each part is again updated.

Result Compilation:

After processing all blocks, the final encrypted binary string is stored.

The Encryption Process with The Proposed Key

In the Encryption Process with the introduced Key, the IDEA algorithm is utilized with the SCKG to encrypt the data. This process takes place through several steps described below:

Text Input Processing:

It reads plaintext, converts it to a8-byte array, and pads this array to ensure its size is a multiple of 8 bytes. This is likely for block processing, as each block is 64 bits (8 bytes).

Block Count Calculation:

It calculates the number of 64-bit blocks in the padded byte array .

Key Extraction and Validation:

The method extracts a series of "K values". It validates the length of these values to ensure they total 832 bits and then splits them into an array of 52 short values.

Block Processing:

Each 64-bit block of the plaintext is processed separately. The method splits each block into four 16-bit values (pValues).

Transformation Rounds:

Each 16-bit value undergoes 8 rounds of transformations using subsets of the K values. After each round, the transformed value is displayed.

Final Transformation:

After the 8 rounds, a final half-round transformation is applied using the last 4 K values.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Result Compilation:

The final binary strings from the transformations of each block are appended together and then displayed.

RESULTS AND DISCUSSION

This section presents the outcomes of the suggested system implementation will be illustrated, analyzed, and discussed. The main goal is to evaluate the performance of the methodologies that are used. A set of 15 tests called (NIST tests) were used to prove the security and confidentiality of the International Data Encryption Algorithm (IDEA) and keys that have been used with it (Traditional and proposed key).Each NIST test relies on a selection procedure to ascertain whether the sequence of bits generated by the algorithm is random .A P- value greater than 0.01 indicates randomness, while a P-value below this threshold indicates non-randomness. The results discussion emphasizes the significance of the research issue as well as states the objectives.

The Results Using Traditional Key

This section contains the findings that we obtained from using the Traditional Key, as described below:

The Results of Traditional Key Generation

A text was tested as Traditional key of IDEA as shown below in Figure 4.1. The size of the entered text must not be less than 128 bits. If it is more than 128 bits, only 128 bits will be taken for processing and the rest will be ignored.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

BabilonUniversity


0100001001100001011000100110100101101100011011110110111001010101011011
0011010010111011001100101011100100111001101101001011101001101001011011
0011011110110111001010101011011100110100101110110011001010111001001110
1101101001011101000100001001100001011000100101110010101010110111001101
0101110110011001010111001001110011011010010111010001000010011000010110
0100110100101101100011011110101001011101100110010101110010011100110101
0010111010001000010011000010110001001101001011011000110111101101110010
0101011011100110010011100110110100101110100010000100110000101100010011
1001011011000110111101101110010101010110111001101001011101100110010101
1100010000100110000101100010011010010110110001101111011011100101010101
0111001101001011101100110010101110010011100110110100101110100110100101
0110001101111011011100101010101101110011010010111011

Figure 1.4 Traditional Key Generation Example

The Results of Cipher Text Using Traditional Key

The text "Babilon University" was employed as the algorithm's traditional key Because it performed well during evaluation, it was applied to the plaintext below as shown by the following:

("However difficult life may seem,

there is always something you can do and succeed at.")

Figure 1.5 Using the Traditional Key in IDEA to apply to certain sentence in English

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Performance Evaluation using NIST with Traditional Key

The text that were entered as IDEA's Traditional keys were assessed using the NIST tests as follows:

Table (4.1): Outcomes of the NIST Tests for Traditional Key "BabilonUniversity"

NIST Tests for Traditional Key "BabilonUniversity"		
Test type	Value of the P-	Result
Frequency Test (Monobit)	0.2385025522723	Succeeded
Frequency Test within a Block	0.9933477857526	Succeeded
Run Test	0.0000000092773	Failed
Longest Run of Ones in a Block	-1.0000000000000	Failed
Binary Matrix Rank Test	0.0000000000000	Failed
Discrete Fourier Transform (Spectral) Test	0.0011742905785	Failed
Non-Overlapping Template Matching Test	0.9937777939478	Succeeded
Overlapping Template Matching Test	-1.0000000000000	Failed
Maurer's Universal Statistical test	-1.0000000000000	Failed
Linear Complexity Test	0.0000000000000	Failed
Serial test	0.0000000000000	Failed
Approximate Entropy Test	0.5132294224405	Succeeded
Cumulative Sums Test	0.4761932998507	Succeeded
Random Excursions Test	0.9859305706853	Succeeded
Random Excursions Variant Test	0.7750075826013	Succeeded

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Performance Evaluation using NIST on Cipher Text with Traditional Key

The ciphertext are evaluated by using NIST Tests below, as shown:

Table (4.2): Results of the NIST Tests for Cipher Text with Traditional Key.

NIST Tests for Cipher Text with Traditional Key		
Test type	Value of the P-	Result
Frequency Test (Monobit)	0.2786604948992	Succeeded
Frequency Test within a Block	0.7587359016863	Succeeded
Run Test	0.4234028849251	Succeeded
Longest Run of Ones in a Block	0.0044814588055	Failed
Binary Matrix Rank Test	-1.0000000000000	Failed
Discrete Fourier Transform (Spectral) Test	0.0010079716919	Failed
Non-Overlapping Template Matching Test	0.9987080223065	Succeeded
Overlapping Template Matching Test	0.0000000000000	Failed
Maurer's Universal Statistical test	-1.0000000000000	Failed
Linear Complexity Test	-1.0000000000000	Failed
Serial test	0.0000000000000	Failed
Approximate Entropy Test	1.0000000000000	Succeeded
Cumulative Sums Test	0.3927319624915	Succeeded
Random Excursions Test	0.0156094161003	Succeeded
Random Excursions Variant Test	0.3495748061233	Succeeded

The Results Using Proposed Key

The results are present in this section, they are obtained from using the Proposed Key, as described below:

The Results of Proposed Chaos Key Generation

The proposed hybrid chaotic system is used as a chaos keys generator to generate random numbers. This system contains two chaos map: Tow dimension Cat map and Tow dimension Henon map. These two maps merge to get 832 bits Key. When applying x_i=x_m= 0.12, y_i=y_m = 0.15, we achieve the key below as **Figure (1.6)**:

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية
ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

11110110010100101010000101001111000111101111010111100011001111110010100111
00100111110111000100010111001110010100110100001011111111000110101000101101
01111010100101111110101111001101011000111111011111000110100000001100110000
00101111001011010011011001001111111110001101101101110110000001111000010011
10000001110100000011111111101100010111000100100001011100111001010100110101
11001100111111011111111100000100011101100100101010101100000000110001100011
11111000100111010101101010110101010111001111010111011100011000111111111000
11101010010010000100010011000110110011000110111001001111110110110011011101
1001000110101111000111000100110111011101001111111110000111011111111000110101
10101100111001000000101010000010111111011111010100110110101101100010110010
10100010100011100110001111110000011010000101101101011110010010000111001100
0110100110001111111

Figure (1.6): Proposed Key Generation Example

These initial values were chosen to generate the proposed key **.**

The Results of Cipher Text Using Proposed Key

The initial values **"x_i=x_m= 0.12, y_i=y_m = 0.15"** were employed to produce the suggested key in the algorithm because of its excellent results during assessment, and it was applied to the plaintexts below, as demonstrated**:**

-

("However difficult life may seem,

there is always something you can do and succeed at.")

00110101011111000011011110110000001110011000110010010000101101001011010101
11110010111011101100000100000000000110000110001101101000100110001111001011
10111011000001010000100011000010100000110100101101010111110011110111101100
00000100001000110000010000101101001001010101111100011101111011000011100000
10001100001010000011010001001001011111000111011110110000111110010000110001
00110010110100001100001111110000101001101100000100000000000110001101000011
01001110011111111100111110011011000010010100100011001010010100110100101101
0101111100111110011011000000111001000011001011000010110100

Figure (1.7): Using the proposed key in IDEA to apply to a few English sentences

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Performance Evaluation using NIST with Proposed Key

The proposed key of IDEA that was generated depending on the initial values was evaluated by NIST tests as shown below:

Table (4.3): Outcomes of the NIST Tests for suggested Key when x_i=x_m= 0.12, y_i=y_m = 0.15.

NIST Tests for Proposed Key when x_i=x_m= 0.12, y_i=y_m = 0.15.		
Type of the test	Value of the P-	Outcomes
Frequency Test (Monobit)	0.0183996528612	Succeeded
Frequency Test within a Block	0.3355392599514	Succeeded
Run Test	0.2575090390041	Succeeded
Longest Run of Ones in a Block	0.0969654135488	Succeeded
Binary Matrix Rank Test	-1.0000000000000	Failed
Discrete Fourier Transform (Spectral) Test	0.0219851032481	Succeeded
Non-Overlapping Template Matching Test	0.7978446507760	Succeeded
Overlapping Template Matching Test	0.0000000000000	Failed
Maurer's Universal Statistical test	-1.0000000000000	Failed
Linear Complexity Test	-1.0000000000000	Failed
Serial test	0.1778811935725	Succeeded
Approximate Entropy Test	0.9999999996877	Succeeded
Cumulative Sums Test	0.0276728587809	Succeeded
Random Excursions Test	0.9625657732473	Succeeded
Random Excursions Variant Test	0.3545394797735	Succeeded

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Performance Evaluation using NIST on Cipher Text with Proposed Key

The ciphertexts presented are assessed by using NIST Tests listed below, as indicated:

Table (4.4): Results of the NIST Tests for Cipher Text 1 with Proposed Key.

NIST Tests for Cipher Text with Proposed Key		
Type of the test	Value of the P-	Outcomes
Frequency Test (Monobit)	0.0552802925860	Succeeded
Frequency Test within a Block	0.3315754312859	Succeeded
Run Test	0.1500240002822	Succeeded
Longest Run of Ones in a Block	0.0438427815953	Succeeded
Binary Matrix Rank Test	-1.0000000000000	Failed
Discrete Fourier Transform (Spectral) Test	0.0786023168906	Succeeded
Non-Overlapping Template Matching Test	0.1533397597858	Succeeded
Overlapping Template Matching Test	0.0000000000000	Failed
Maurer's Universal Statistical test	-1.0000000000000	Failed
Linear Complexity Test	-1.0000000000000	Failed
Serial test	0.0000000000000	Failed
Approximate Entropy Test	1.0000000000000	Succeeded
Cumulative Sums Test	0.0744416999386	Succeeded
Random Excursions Test	0.1043232877697	Succeeded
Random Excursions Variant Test	0.9294304154577	Succeeded

The results of the IDEA tests using the suggested and traditional keys were examined and assessed in the preceding pages. The tests demonstrated the following:

The suggested key passed 11 of the 15 tests that were used to evaluate the keys, compared to the Traditional key of IDEA passing just 7. This indicates that the proposed method is superior by 4 tests over the Traditional method of generating keys .

For evaluating the ciphertext, the cipher text with the proposed key passed 10 tests out of the 15 total tests, while with the Traditional key passed only 8 .

The use of two kinds of chaotic maps in the proposed key generation method gives it a high degree of randomness.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية

CONCLUSIONS

After implementing the proposed system, some conclusions that are related to it are assembled:-

The use of a 2D chaotic system in the operation of produce the secret key for the IDEA led to high randomness and unexpected output.

Modification of the IDEA by using the Proposed key rather than the Traditional key made it better suited for use in cryptography systems.

Conflict of interests.

There are no conflicts to declare.

References

1. W. Stallings, *Cryptography and network security*, 7 ed. India: Pearson Education 2017.
2. P. K. Panda and S. Chattopadhyay, "A hybrid security algorithm for RSA cryptosystem," in *4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2017.
3. N. Ferguson, B. Schneier, and T. Kohno, *Cryptography engineering: design principles and practical applications*. New Jersey: John Wiley & Sons, 2011.
4. A. Alabaichi and A. I. Salih, "Enhance security of advance encryption standard algorithm based on key-dependent S-box," in *Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, 2015.
5. G. T. Cayabyab, A. M. Sison, and A. A. Hernandez, "GISKOP: A modified key scheduling operation of international data encryption algorithm using serpent key scheduling," in *Proceedings of the 2nd International Conference on Computing and Big Data*, 2019.
6. H.-S. Chang. "*International Data Encryption Algorithm,*" scribd.com, Sep. 2, 2010 [Online]. Available: https://www.scribd.com/presentation/36792152/IDEA-by-How-Shen-Chang-2004-FALL. [Accessed: Sep. 2, 2010]
7. J. Daemen, R. Govaerts, and J. Vandewalle, "Weak keys for IDEA," in *13th Annual International Cryptology Conference Santa Barbara*, 1994.

8. S. Sheela and S. Sathyanarayana, "Application of chaos theory in data security-a survey," *ACCENTS Transactions on Information Security,* vol. 2, no. 5, Dec. 2016.

9. S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik,* vol. 272, p. 170316, Feb. 2023.

10. N. Abdulraheem and B. M. Nema, "Secure IOT model based on present lightweight modified and chaotic key generator," in *1st. Information Technology To Enhance e-learning and Other Application (IT-ELA)*, 2020.

11. S. Patil and V. Bhusari, "An enhancement in international data encryption algorithm for increasing security," *International Journal of Application or Innovation in Engineering Management,* vol. 3, no. 8, pp. 64-70, Aug. 2014.

12. O. Jallouli, "Chaos-based security under real-time and energy constraints for the Internet of Things," Ph.D. dissertation, University de Nantes, Nantes, France, 2017.

13. M. K. C. Ledda, B. D. Gerardo, and A. A. Hernandez, "Security Evaluation of the Enhanced IDEA Algorithm," in *2nd World Symposium on Communication Engineering (WSCE)*, 2019.

14. Z. Wang *et al.*, "Enabling fairness-aware and privacy-preserving for quality evaluation in vehicular crowdsensing: a decentralized approach," *Security Communication Networks,* vol. 2021, pp. 1-11, Nov. 2021.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

Article
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Vol.32; No.2.| 2024

الخلاصة

مقدمة :

خوارزمية تشفير البيانات الدولية (IDEA) هي خوارزمية تشفير مستخدمة على نطاق واسع وقد أثارت المخاوف بسبب اكتشاف العديد من المفاتيح الضعيفة، كما تم توضيحه في الأبحاث السابقة. تم العثور على هذه المفاتيح الضعيفة، وتحديدًا تلك التي تحتوي على تسلسلات متتالية من أرقام مفردة، لتعيق تطور الخوارزمية وتؤدي إلى تأثير انهيار جليدي بطيء. ولمعالجة نقاط الضعف هذه، يهدف هذا البحث إلى تطوير خوارزمية تشفير محسنة وآمنة من خلال دمج مبادئ نظرية الفوضى في IDEA.

طرق العمل:

الهدف الأساسي هو معالجة نقاط الضعف المرتبطة بعملية إنشاء المفاتيح الخاصة بـ IDEA من خلال الاستفادة من نظرية الفوضى لإنشاء مفاتيح قوية وعشوائية للغاية تحل محل مفاتيح الخوارزمية الضعيفة. تهدف الدراسة أيضًا إلى تقييم الأمان وقوة التشفير لخوارزمية IDEA المحسنة من خلال التقييمات والمقارنات مع الخوارزمية الأصلية.

النتائج:

أظهرت النتائج أن المفتاح المقترح اجتاز 11 اختباراً من إجمالي 15 اختباراً، في حين اجتاز المفتاح التقليدي لـ IDEA 7 اختبارات فقط، مما يدل على أن الطريقة المقترحة تتفوق بـ 4 اختبارات على الطريقة التقليدية في توليد المفاتيح. كما اجتاز نص التشفير بالمفتاح المقترح 10 اختبارات من إجمالي 15 اختبارًا، بينما مع المفتاح التقليدي اجتاز 8 فقط.

الإستنتاجات:

وهذا يدل على تفوق طريقة IDEA المقترحة في التشفير على طريقة IDEA التقليدية.

الكلمات المفتاحية: الخوارزمية التقليدية، الخوارزمية المقترحة، النص المشفر الامن، النظام الفوضوي، المعهد الوطني للمعايير والتكنولوجيا.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية