Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 7, Issue 3, December 2024
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN: 2789-7362

ENHANCE STREAM CIPHER USING MODIFIED FISHER ALGORITHM

Hatem K. Mohammed [1], **Alhamza T. Mohammed** [2], **Mohammed J. Zaiter** [3]
[1,2,3] Middle Technical University (MTU), Electrical Engineering Technical College, Department of Computer Technical Engineering, Al Doura 10022, Baghdad, Iraq
bbc0084@mtu.edu.iq[1], alhamza_tm@mtu.edu.iq[2], mjzaiter@mtu.edu.iq[3]
Corresponding Author: **Mohammed J. Zaiter**
Received:18/07/2024; Revised:04/12/2024; Accepted:24/12/2024
DOI:10.31987/ijict.7.3.293

***Abstract*- Cryptography, being an important science in securing communications networks, is continuously looking for novel ways to strengthen traditional encryption techniques. This study explores the possibilities of improving the Stream Cipher and fortifying it with a Modified Fisher Algorithm (MFA). Hence, the combination of Stream Cipher with Modified Fisher Algorithm (SCwMFA) is more secure than each cipher alone. Where the Stream Cipher is regarded as a powerful approach that uses binary form instead of characters with MFA to increase the strength of the needed key. This combination offers a good level of security. Experimental results reveal that the suggested combining algorithms based on the Index of Coincidence (IoC) metric outperforms the Stream Cipher with The Traditional Fisher-Algorithm (SCwTFA) in terms of security with increasing cryptanalysis complexity.**

keywords: **Stream cipher, Fisher–yates algorithms, Index of Coincidence, Encryption, Decryption, ASCII.**

I. INTRODUCTION

In recent years, the rapid advancement of communication technologies has increased the necessity for individuals to connect across insecure networks, as has the number of attacks on computers and people. Consequently, information security measures such as integrity, secrecy, and authentication have been recommended. Where encryption techniques are effective tools for safeguarding sensitive data and preventing unauthorized users from accessing the original content. Hence, Stream Ciphers beat traditional security algorithms in terms of performance, cost, and complexity [1].

Several research attempts to improve the security of Stream Ciphers by combining it with another algorithm. Where the Stream Cipher is a symmetric cryptosystem that provides hardware-based approaches with increased speed and scalability [2]. Stream Ciphers are best suited for most applications when the text input is either undefined or continuous. Stream Ciphers are lightweight, quick, low power consumption, and appropriate for devices with limited resources [3, 4]. Self-synchronous stream encryption is based on either plaintext or prior ciphertext data, resulting in a faster deployment of stream security solutions [5]. To prevent attackers from swiftly deciphering the Stream Cipher, the key must be random. To create a random key, there are several approaches. A pseudo-random number generator is the most well-known method (PRNG). The PRNG standard offers a high-performance speed that produces unexpected and random sequences [6].

Therefore, the study in [7], suggested building a key generator using the sensors included in Android smartphones. It was developed by using a variety of sensors to produce a key that functions as a True Random Number Generator (TRNG). The study in [8], developed an innovative key generator derived from the chaotic system. Authors used this technique to encrypt pictures by creating random numbers with a Pseudo-Chaotic Number Generator (PCNG). A robust key stream. Different privacy and security features can be used to assess blockchain-based electronic healthcare industry 4.0 solutions.

ISSN:2222-758X
e-ISSN: 2789-7362

Moreover, blockchain technology has been used in earlier research projects to develop electronic healthcare 4.0 systems that integrate security and privacy characteristics [9]. There are several issues with the techniques used to encrypt video and image streams, and there are numerous approaches for encrypting images. Conventional methods of data encryption are only effective when used to encode textual data. Recently, the scientific world has made a payment close focus on DNA studies [10]. Encryption techniques are categorized into two main types: Block Cipher and Stream Cipher. In Block Cipher, encryption is performed on a block level, meaning that each block of data is encrypted bit by bit. On the other hand, in Stream Cipher, encryption is done on a bit-by-bit basis using a safe key generator [11].

The researchers in [12], introduced a novel method for reversible data hiding in encrypted images. This method utilizes multiple secret sharing as the underlying cipher and employs lightweight cryptographic algorithms to compress and generate a Single Shared Key (SOK). The study in [13], examined the difficulties and problems associated with key generation in WSN by introducing the notion of asymmetric key generation.

Overall, these studies highlight the significance of utilizing cryptographic approaches to safeguard the specified systems. A hybrid method that leverages genetic traits to generate a key and tests its randomness using recognized methods is offered for more secure encryption, faster execution, and cost calculation. In a new method, the key was camouflaged in the ciphertext before transmission to ensure its integrity. The proposed method avoided previous approach flaws with the genetic algorithm. A random key was generated using the rand function, considering the length of the encrypted text. Following the established conditions, each generation member was examined for randomness [14]. Suggested enhancing the SNOW-3G algorithm by incorporating a super-chaos generator. To enhance the unpredictability of the generated key sequence [15]. The study in [16], suggested employing enhanced identity-based encryption to generate protected keys for cloud systems, ensuring the concealment of the consumer's identity even if the attacker manages to decrypt the keys or data.

However, the most recent research on Stream Ciphers has taken a variety of methods, ranging from improving algorithm security to increasing the complexity of cryptanalytic techniques by integrating them with other modern algorithms. Therefore, this paper provides a combination technique Stream Cipher with Modified Fisher Algorithm (SCwMFA). The Stream Cipher's present security method serves as the foundation for this combination, which is improved with Modified Fisher Algorithm (MFA) to provide the keys required to increase encryption strength. As a result, the MFA approach creates random keys using every character and symbol on the keyboard, making encryption more secure and resistant to cryptographic assaults.

II. CONTRIBUTIONS

This paper provides several important contributions to the theory and analysis of Stream Cipher security. First, propose a new method called Modified Fisher Algorithm (MFA) which is an improvement on the traditional MFA with an increased set of characters from the ASCII which includes the small letters, capital letters, and numeral values as well as the special symbols. The above-mentioned change increases the key space in addition to the randomness thus enhancing the security and the encryption from cryptographic attacks. Second, a process of examining the improved strength of the encryption

ISSN:2222-758X
e-ISSN: 2789-7362

is shown that occurs when the MFA is combined with a Stream Cipher to produce keys that are less easily guessed or mimicked. Finaly, the results of this experiments proved the effectiveness of the SCwMFA over traditional methods, especially in terms of key complexity and security as measured by the Index of Coincidence (IoC).

III. PROPOSED TECHNIQUE

This project aims to improve data security by integrating the SCwMFA with Stream Cipher. A dependable technique for encrypting a stream of characters, numerals, and symbols is offered by Stream Ciphers. Furthermore, instead of using the standard Fisher approach, which is based solely on simple plaintext, the MFA generates a random key based on all characters and symbols on the computer's keyboard to boost security. Fig. 1 depicts the specifics of the suggested SCwMFA.

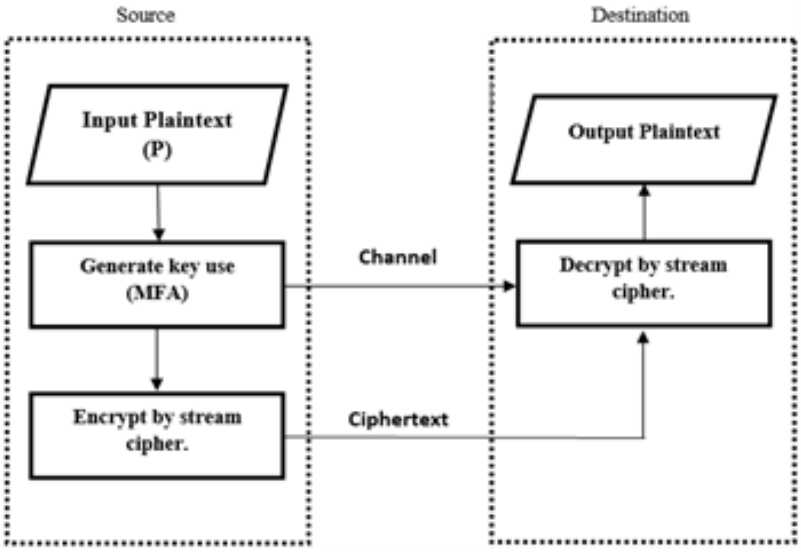

Figure 1: Proposed Works.

Traditional Fisher Algorithm Stream Cipher (SCwTFA)The Traditional Fisher Algorithm (TFA) is predicated on an algorithm that produces the necessary keys by randomly permuting plaintext characters. Hence, a Stream Cipher is an encryption technique that manipulates data size bits or bytes to encrypt plaintext into ciphertext, as shown in Fig. 2.

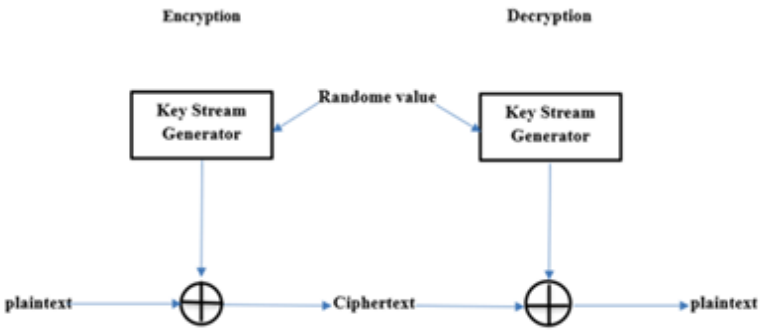

Figure 2: Stream Cipher.

Table I shows the encryption results by using Stream SCwTFA. Where the plaintext is "I meet you at 6:30 PM". The traditional Fisher algorithm is used to generate the required key, which is determined only by the characters in the plaintext. Where the characters the plaintext and the generated key are transformed into an ASCII value and subsequently to the corresponding binary form. Encrypting these characters using the Stream Cipher equation, where the cipher text is formed using the plaintext is "XORed" with the keystream, one bit at a time. as the following equation:

$$C = P_{\text{bin}} \otimes K_{\text{bin}} \tag{1}$$

At the destination, the decryption procedure decrypts the cipher text and keystream to return the original plain text (the same keystream will be used for encryption).

TABLE I
Encryption by Stream Cipher with Traditional Fisher Algorithm (SCwTFA)

Plaintext	I	m	e	e	t	y	o	u	a	t	6	:	3	0	P	M
ASCII (dec)	73	109	101	101	116	121	111	117	97	116	54	85	51	48	80	77
Binary Conversion	0100 1001	0110 1101	0110 0101	0110 0101	0111 0100	0111 1001	0110 1111	0111 0101	0110 0001	0111 0100	0011 0110	0011 1010	0011 0011	0011 0000	0101 0000	0100 1101
Key Generator	t	u	6	o	e	y	a	e	I	:	M	0	P	t	3	m
ASCII (dec)	116	117	54	111	101	121	97	101	73	85	77	48	80	116	51	109
Binary Conversion	0111 0100	0111 0101	0011 0110	0110 1111	0110 0101	0111 1001	0110 0001	0110 0101	0100 1001	0011 1010	0100 1101	0011 0000	0101 0000	0111 0100	0011 0011	0110 1101
$C = P_{\text{bin}} \oplus K_{\text{bin}}$	0011 1101	0001 1000	0001 1100	0000 1010	0001 0001	0000 0000	0000 1110	0001 0000	0010 1000	0010 0001	0111 1011	0110 0101	0110 0011	0100 0100	0110 0011	0010 0000
ASCII (dec)	61	24	28	10	17	0	14	16	40	33	123	101	99	68	99	32
Ciphertext	=	↑	∟	♣	◁	space	♯	▷	(	!	{	e	c	D	c	O

Table II shows the Stream Cipher's decryption results and the plaintext that was obtained.

In SCwMFA, the MFA was utilized to improve and strengthen key for the Stream Cipher. The MFA proposed in this work to generates a random key of 94 characters in length that includes all small and capital letters, numerals, and symbols of the computer's keyboard to provide the required key, and if the plaintext exceeds 94 characters, the key is repeated until

ISSN:2222-758X
e-ISSN: 2789-7362

TABLE II
Decryption by Stream Cipher with Traditional Fisher Algorithm (SCwTFA)

Ciphertext	=	↑	∟	♣	◁	space	♯	▷	(	!	{	e	c	D	c	Ö
ASCII (dec)	61	24	28	10	17	0	14	16	40	33	123	101	99	68	99	32
Binary Conversion	0010 0010	0000 1000	0001 1100	0000 1110	0001 0001	0000 0000	0000 0100	0001 0000	0001 1000	0001 1111	0101 0010	0010 1100	0101 1011	0101 0101	0010 1001	0010 0110
Key Generator	t	u	6	o	e	y	a	e	I	:	M	0	P	t	3	m
ASCII (dec)	116	117	54	111	101	121	97	101	73	85	77	48	80	116	51	109
Binary Conversion	0111 0100	0111 0101	0011 0110	0110 1111	0110 0101	0111 1001	0110 0001	0110 0101	0100 1001	0011 1010	0100 1101	0011 0000	0101 0000	0111 0100	0011 0011	0110 1101
$P = C_{\text{bin}} \oplus K_{\text{bin}}$	0100 1001	0110 1101	0110 0101	0110 0101	0111 0100	0111 1001	0110 1111	0111 0101	0110 0001	0111 0100	0011 0110	0011 1010	0011 0011	0011 0000	0101 0000	0100 1101
ASCII (dec)	73	109	101	101	116	121	111	117	97	116	54	85	51	48	80	77
Plaintext	I	m	e	e	t	y	o	u	a	t	6	:	3	0	P	M

the plaintext is covered. Fig. 3 depicts how the MFA algorithm works.

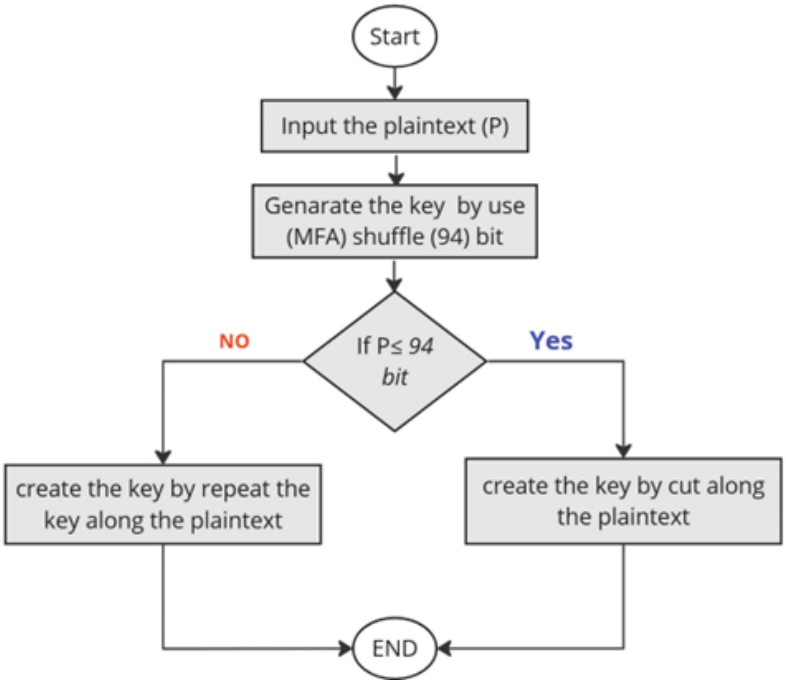

Figure 3: The proposed flowchart of MFA.

The modification that was previously applied to the algorithm was based on generating a random key based on the letters of the plain text to be encrypted, while in this study the proposed algorithm based on all the letters, symbols, and numbers on the computer keyboard based on the ASCII decimal table, which gives a strong character to the shape of the key in terms of the strength of the message encryption, and on the other hand the difficulty of predicting the key that is difficult to access. The Fisher algorithm takes sequential stages are:

1) To shuffle an array a of n elements (indices $0 \ldots n-1$):

ISSN:2222-758X
e-ISSN: 2789-7362

2) For i from $n-1$ down to 1, do:
3) Select a random integer j such that $0 \leq j \leq i$.
4) Exchange $a[j]$ and $a[i]$.
5) end

This method works by calculating the length of the text to be encrypted, subtracting one element from the overall length of the plain text, and selecting a random position from one of the remaining elements in the text. This procedure is repeated until the final bit in the text. This approach creates a random key for each transmission operation, resulting in a unique key that is difficult to access and anticipate.

Table III displays the encryption results of the SCwMFA. Where the produced key via MFA is compared to TFA, it can be seen how much stronger the key has become, Increasing the level of unpredictability for potential attackers to hinder their ability to anticipate the encryption key. To extract the ciphertext, convert the resulting binary numbers to their ASCII equivalents and then characters.

TABLE III
Encryption by Stream Cipher with Modified Fisher Algorithm (SCwMFA).)

Plaintext	I	m	e	e	t	y	o	u	a	t	6	:	3	0	P	M
ASCII (dec)	73	109	101	101	116	121	111	117	97	116	54	85	51	48	80	77
Binary Conversion	0100 1001	1101 0001	0110 0101	0110 0101	0111 0100	0111 1001	0110 1111	0111 0101	0110 0001	0111 0100	0011 0110	0101 0101	0011 0011	0011 0000	0101 0000	0100 1101
Key Generator	!	v	-	*		?	*	8	>	]	%	c	7	+	B	/
ASCII (dec)	33	86	45	42	123	63	42	56	62	93	37	67	55	43	66	47
Binary Conversion	0010 0001	0101 0110	0010 1101	0010 1010	0111 1011	0011 1111	0010 1010	0011 1000	0011 1110	0101 1101	0010 0101	0100 0011	0011 0111	0010 1011	0100 0010	0010 1111
$C = P_{\text{bin}} \oplus K_{\text{bin}}$	0110 1000	1000 0111	0100 1000	0100 1111	0000 1111	0101 0000	0100 0101	0100 1101	0111 1010	0010 1001	0001 0011	0001 0110	0000 0100	0001 1011	0001 0010	0110 0010
ASCII (dec)	104	135	72	79	15	80	69	77	122	41	9	22	4	27	18	98
Ciphertext	h	ζ	H	o	⊗	P	E	M	z	)	○	-	◇	←	↕	b

Finally, Table IV displays the decryption results for the SCwMFA and the retrieved plaintext.

TABLE IV
Decryption by Stream Cipher with Modified Fisher Algorithm (SCwMFA)

Ciphertext	h	ζ	H	o	⊗	P	E	M	z	)	○	-	◇	←	↕	b
ASCII (dec)	104	135	72	79	15	80	69	77	122	41	9	22	4	27	18	98
Binary Conversion	0110 1000	1000 0111	0100 1000	0100 1111	0000 1111	0101 0000	0100 0101	0100 1101	0111 1010	0010 1001	0001 0011	0001 0110	0000 0100	0001 1011	0001 0010	0110 0010
Key Generator	!	v	–	*		?	*	8	>	]	%	c	7	+	B	/
ASCII (dec)	33	86	45	42	123	63	42	56	62	93	37	67	55	43	66	47
Binary Conversion	0010 000	0101 0110	0010 1101	0010 1010	0111 1011	0011 1111	0010 1010	0011 1000	0011 1110	0101 1101	0010 0101	0100 0011	0011 0111	0010 1011	0100 0010	0010 1111
$P = C_{\text{bin}} \oplus K_{\text{bin}}$	0100 1001	1101 0001	0110 0101	0110 0101	0111 0100	0111 1001	0110 1111	0111 0101	0110 0001	0111 0100	0011 0110	0101 0101	0011 0011	0011 0000	0101 0000	0100 1101
ASCII (dec)	73	109	101	101	116	121	111	117	97	116	54	85	51	48	80	77
Plaintext	I	m	e	e	t	y	o	u	a	t	6	:	3	0	P	M

This improvement to the Fisher Algorithm increases key generation by adding all the small cases, capital cases, numerals, as well as symbols on the ASCII decimal table to 94 characters. Unlike the TFA, which derives keys following the respective

ISSN:2222-758X
e-ISSN: 2789-7362

plaintext character, and then forms an array of keys knowing that most of the array locations will have similar keys to detrimental the code, this modification makes the key the more complicated and trickier. Hence, the usages of a larger set of characters means that the aggregate key is more impenetrable to frequency analysis and all forms of cryptographic assault. The process incorporates Fishers shuffle stages with a pseudo-random selection mechanism that adds randomization and cryptographic strength to the operand key.

This modification enhances the security of Stream Ciphers by having a separate generator for the key and the plaintext so that each time a cipher text is produced a different and more random key is generated. The broader the key space, the greater the number of possibilities, resulting in higher entropy and making it more difficult for an attacker to guess or replicate the key. Thus, utilizing the proposed flowchart, the character selection range and randomizing functions lead to the creation of a much stronger encryption key and therefore, the overall security of the encryption process grows as a response to the contemporary cryptanalytic methods and approaches.

IV. DETAILS OF MFA

A. Mathematical Foundation of MFA

The only modification made to the Fisher Algorithm is concretized in the expansion of the key generation process to all the characters belonging to the ASCII decimal table. This consists of small case alphabets (a-z), Capital case alphabets (A-Z), numerals (0-9), and other special characters and these are totaling to make 94 characters. This makes the importance of the keys much larger than the common Fisher Algorithm where only a limited number of characters based on the plaintext is chosen.

The operational foundation of the MFA is conceptualized in the Fisher-Yates shuffle, which is an already-established technique of shuffling a sequence of items with full randomness. The modification occurs in the first step in which a list of candidates for character replacement is wider, including many ASCII characters. The latter consists of a sequence of these characters which have been shuffled by a Pseudo-Random Number Generator (PRNG) so that MFA has a unique key for each encryption session.

B. Algorithmic Steps of MFA

The algorithmic steps of the MFA begin with the selection of a character set based on the ASCII decimal table, which includes 94 characters: letters in lower case, letters in upper case, numbers, and special characters. The next operation is the Fisher-Yates shuffle method in which each character in the character set is exchanged with another arbitrarily until all elements are shuffled. Subsequently, the key stream is derived from the characters of the shuffled array; if the Plaintext is longer than the key set, which is 94 characters, the key stream runs through the Plaintext again. This ensures that the encryption key all the time remains a random one. Finally, the generated key in binary form is logically XORed with the binary form of the plaintext to get the ciphertext, which is reminiscent of the Stream Cipher techniques, but the additional

ISSN:2222-758X
e-ISSN: 2789-7362

random key generation makes the present cipher stronger than the conventional approaches.

C. Comparison of Key Generation: TFA vs. MFA

A direct comparison between the TFA and the MFA is essential to understand the improvements in key strength. The Table V summarizes the key differences the algorithms.

TABLE V
Comparison of TFA and MFA

Feature	Traditional Fisher Algorithm (TFA)	Modified Fisher Algorithm (MFA)
Character Set	Based only on characters in the plaintext	Includes all ASCII characters (94 characters: letters, numbers, symbols)
Key Space Size	Limited by the size of the plaintext	Vastly expanded key space due to the inclusion of 94 characters
Key Randomness	Limited by plaintext patterns, leading to potential predictability	Highly randomized, reducing predictability and increasing complexity
Key Generation Process	Shuffling of characters based on plaintext	Expanded shuffling with pseudo-random number generator (PRNG) using full ASCII set
Encryption Strength	Weaker, due to reduced randomness and keyspace	Stronger, due to higher entropy and unpredictability

V. Index of Coincidence

The IoC is a metric that measures the similarity between the frequency distribution of characters in plaintext and ciphertext. Where it represents the frequency of a letter occurring in the given ciphertext message. IoC refers to measures of the likelihood of drawing two matched letters by randomly picking two letters from a given text. The IoC is calculated by using the following formula [17, 18]:

$$\text{IoC} = \frac{\sum_{i=1}^{j} f_i(f_i - 1)}{n(n-1)} \tag{2}$$

Here, n represents the total length of the text, which is the same as the number of characters, and the i represents the iteration counter which it has ranges from 1 to 26, corresponding to the 26 English alphabets.
To make the computation more straightforward, the authors in [19] suggested to use an estimate of the key length [19]. To determine the length of the applied key, the Friedman test in [19] is utilized. An estimation of the key length of the keyword is created by applying Friedman's equation which is presented.

$$\text{Key length} = \frac{0.027\,n}{\text{IC}\,(n-1) - 0.038 + 0.065} \tag{3}$$

ISSN:2222-758X
e-ISSN: 2789-7362

VI. RESULTS AND DISCUSSIONS

The comparison between SCwTFA and the SCwMFA is shown in Table VI, in terms of key strength and the IoC. Where results demonstrates that SCwMFA is more efficient and powerful than SCwTFA. This is due to the complexity of the SCwMFA encryption key, which includes all of the letters, numbers, and symbols present on the computer keyboard in the ASCII decimal system.

TABLE VI
Comparison of IoC (Index of Coincidence) for SCwTFA and SCwMFA

No. of Characters	IoC (SCwTFA)	IoC (SCwMFA)
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0.00654	0
10	0.00952	0
11	0.01186	0
12	0.01282	0.01182
13	0.01471	0.00952
14	0.01468	0.00833
15	0.01515	0.00735
16	0.01754	0.00725
17	0.01818	0.00654
18	0.02222	0.00535
19	0.02633	0.00526
20	0.03261	0.00476
21	0.03333	0.00433
22	0.03571	0.00362
23	0.03636	0.00342
24	0.04545	0.00333
25	0.06667	0.00308

A. Comparison of This Study with Earlier Studies

This subsection involved a comparison to assess the robustness of the encryption. The strategies employed in this research resulted in a drop of the IoC value to 0.003, providing an indicator of the robustness of the encryption implemented in

this study based on the applied procedure. Fig.4 provides a valuable comparative overview of all studies with this study.

Figure 4: Analyses result.

Also, Table VI presents a comparison between the results obtained from existing studies and the values obtained from this study.

TABLE VII
Comparison of this study with previous studies

Ref.	year	Approach	IoCD
[20]	2021	(TFA)	0.03
[21]	2023	(TFA)	0.0420
[22]	2023	(TFA)	0.05
[23]	2024	(TFA)	0.04502
24]	2021	(TFA)	0.0246154
[25]	2023	(TFA)	0.0236
this Proposed	2024	(MFA)	0.00362

The table compares the performance of various studies based on their approaches and Indicators of Compromise (IoC) values. All prior works [20â25] utilize the TFA between 2021 and 2024, achieving IoC values ranging from 0.0236 to 0.05. Among these, the lowest IoC value of 0.0236 was recorded in 2023 [25], while the highest was 0.05 in the same year [22]. In contrast, this proposed approach (MFA) in 2024 significantly outperforms previous studies, achieving a notably lower IoC value of 0.00362. This highlights the improved effectiveness and precision of proposed method compared to traditional approaches.

Finally, the comparison of the existing Stream Cipher with previous studies using a standard key with a key enhanced by the MFA highlights the importance of key modification methods in influencing cryptographic strength and security.

ISSN:2222-758X
e-ISSN: 2789-7362

Using a conventional key for encryption has weaknesses including being predictable and having a pattern that repeats over time. Incorporating MFA into the existing Stream Cipher performs a dynamic key-changing process based on Fisher sequences, which enhances cryptographic strength. Implementing MFA enhances the ability of the cipher to withstand typical cryptanalysis methods, especially frequency-based attacks, and enhances the overall unpredictability of the encryption process. The significant improvement in security from using MFA highlights the need for improved key modification methods in strengthening cryptographic protocols against changing threats.

VII. CONCLUSIONS

Recently, an improved method of Stream Cipher known as SCwMFA strengthens the cipher by using the fishesâ algorithm in addition to the conventional Stream Cipher method. The proposed model improves key generation by increasing the number of characters in the alphabet set to all ASCII, including all small letters, all capital letters, all digits, and other additional symbols. It also leads to the critical guarantee of a lengthier and less predictable key and hence makes an impressive add-up to the code from attacks like the frequency analysis.

The model's steps involve, the presented encryption approach can be divided into four steps. First, choosing a character from the ASCII decimal table; second, shuffling the characters in the array according to the Fisher-Yates shuffle method; third, generating the desired key stream by selecting characters from the shuffled array and repeating the stream until it reaches the length of the plaintext; and, fourth, the binary representation of plaintext is then XOR-ed with the generated key to form the ciphertext. Hypothesis evaluation substantiates the hypothesis that the proposed SCwMFA would provide higher performance than the traditional methodologies by using the IoC performance measure. The analysis of IoC infers that within the SCwMFA there is a poor susceptibility to cryptanalysis thereby improving the strength of encryption than the one that was seen in the Stream Cipher with SCwTFA.

Future research on the SCwMFA could explore three key directions: reinforcing the methodology of creating complex "keys" using other significant techniques like the chaotic systems or machine learning for the sake of attaining a more and more improbable value of the "key". Testing the effectiveness of the model when implemented in real-world applications such as for security in communications and smart devices as well as analyzing the possibility and feasibility of its scalability. Extending cryptanalysis up to the next level, from the IoC to comprehensive cryptographic evaluations of the model for its security against the new types of cryptography threats including the threats from quantum computers.

Funding

None

ACKNOWLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest

REFERENCES

[1] L. Jiao, Y. Hao, and D. Feng, "Stream Cipher designs: a review," Sci. China Inf. Sci., vol. 63, no. 3, p. 131101, Mar. 2020, doi: 10.1007/s11432-018-9929-x.

[2] R. Ananth and N. S. Ramaiah, "An exhaustive review of the Stream Ciphers and their performance analysis," Int. J. Reconfigurable Embed. Syst. IJRES, vol. 13, no. 2, p. 360, Jul. 2024, doi: 10.11591/ijres.v13.i2.pp360-371.
[3] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and Y. Papaefstathiou, "A survey of lightweight Stream Ciphers for embedded systems: A survey of lightweight Stream Ciphers for embedded systems," Secur. Commun. Netw., vol. 9, no. 10, pp. 1226–1246, Jul. 2016, doi: 10.1002/sec.1399.
[4] A. Perez-Resa, M. Garcia-Bosque, C. Sanchez-Azqueta, and S. Celma, "A new method for format-preserving encryption in high-data-rate communications," IEEE Access, vol. 8, pp. 21003-21016, 2020.
[5] L. Jiao, Y. Hao, and D. Feng, "Stream Cipher designs: a review," Sci. China Inf. Sci., vol. 63, no. 3, p. 131101, Mar. 2020, doi: 10.1007/s11432-018-9929-x.
[6] O. Salhab, N. Jweihan, M. A. Jodeh, M. Abutaha, and M. Farajallah, "SURVEY PAPER: PSEUDO RANDOM NUMBER GENERATORS AND SECURITY TESTS.," 2018, Accessed: Jun. 24, 2024. [Online]. Available: https://scholar.ppu.edu/handle/123456789/8187
[7] A. Marghescu, G. Teseleanu, and P. Svasta, "Cryptographic key generator candidates based on smartphone built-in sensors," in 2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME), IEEE, 2014, pp. 239-243. Accessed: Jun. 24, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6967037/
[8] O. Jallouli, S. El Assad, and M. Chetto, "Robust chaos-based stream-cipher for secure public communication channels," in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2016, pp. 23-26. Accessed: Jun. 24, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7856658/
[9] S. Qahtan, K. Yatim, M. H. Osman, H. Zulzalil, and M. L. M. Zakaria, "A Decision Cloud Ranking Approach Based on Privacy and Security in Blockchain E-Health Industry 4.0 Systems," J. Tech., vol. 5, no. 4, pp. 1-15, 2023.
[10] S. T. Ahmed, D. A. Hammond, R. F. Chisab, and N. B. H. Ismail, "Medical Image Encryption and Decryption Based on DNA: A Survey," J. Tech., vol. 5, no. 3, pp. 116-128, 2023.
[11] M. H. Taha and J. M. Al-Tuwaijari, "Improvement of Chacha20 algorithm based on a tent and Chebyshev chaotic maps," Iraqi J. Sci., pp. 2029-2039, 2021.
[12] Y. C. Chen, T. H. Hung, S.-H. Hsieh, and C.-W. Shiu, "A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 12, pp. 3332-3343, 2019.
[13] A. Moradkhani, A. Broumandnia, and S. J. Mirabedini, "Security management of wireless sensors network in industrial application," Int. J. Nonlinear Anal. Appl., vol. 14, no. 1, pp. 1125-1132, 2023.
[14] S. A. Shawkat, N. Tagougui, and M. Kherallah, "Optimization-based pseudo-random key generation for fast encryption scheme," Bull. Electr. Eng. Inform., vol. 12, no. 2, pp. 1007-1018, 2023.
[15] C. Shen et al., "An FPGA design and implementation of 4G network 286security algorithm based on SNOW3G," in Proc. IEEE 19th Int. Conf. 287Softw. Qual. Rel. Security Compan. (QRS-C), 2019, pp. 387-392.
[16] "Retracted: An Improved Secure Key Generation Using Enhanced Identity-Based Encryption for Cloud Computing in Large-Scale 5G," Wirel. Commun. Mob. Comput., vol. 2023, pp. 1-1, Aug. 2023, doi: 10.1155/2023/9789476.
[17] Bhatia, D., Dave, M. (2021). "Elliptic Curve Layered: A Secure Polyalphabetic Vignere Cryptographic Algorithm for Textual Data". Journal of Scientific Research, 65(1), pp. 222-229.
[18] Muhammed, A. J., Tsegaye, G. G., Woldegiorgis, T. A. (2024). "Enhancing the Security of Vigenere and Polybius Hybrid Cryptography System using Modified Linear Congruential Generation Algorithm".
[19] D. Bhatia and M. Dave, "Elliptic Curve Layered: A Secure Polyalphabetic Vigenere Cryptographic Algorithm for Textual Data," J. Sci. Res., vol. 65, no. 1, pp. 222-229, 2021.
[20] J. P. G. Perez et al., "A Modified Key Generation Scheme of Vigenere Cipher Algorithm using Pseudo-Random Number and Alphabet Extension," in 2021 7th International Conference on Computer and Communications (ICCC), IEEE,2021, pp.565-569. Accessed: Mar .31.2024.
[21] C. Millichap, Y. Yau, A. Pate, and M. Carns, "Modifying twist algorithms for determining the key length of a Vigenere cipher," Cryptologic, pp. 1-16, Dec. 2023, Doi: 10.1080/01611194.2023.2275583.
[22] C. L. Tumazar, B. D. Elevazo, V. A. Agustin, J. C. Morano, and M. C. R. Blanco, "Enhancement of the 95x95 Vigenere Cipher Using a 3D Tabula Recta and a New Key Generation Technique in Application to Database Encryption", Accessed: Mar. 31, 2024. [Online]. Available: https://uijrt.com/articles/v4/i8/UIJRTV4I80013.pdf
[23] A. J. Muhammed, G. G. Tsegaye, and T. A. Woldegiorgis, "Enhancing the Security of Vigenere and Polybius Hybrid Cryptography System using Modified Linear Congruential Generation Algorithm," 2024, Accessed: Mar. 31, 2024. [Online]. Available: https://www.researchsquare.com/article/rs-3848010/latest
[24] D. Bhatia and M. Dave, "Elliptic Curve Layered: A Secure Polyalphabetic Vigenere Cryptographic Algorithm for Textual Data," J. Sci. Res., vol. 65, no. 1, pp. 222-229, 2021.
[25] K. Intani, G. Wulandari, H. Hasanah, I. L. Syarifudin, and E. M. C. Brillian, "Meningkatkan Keamanan Pesan Rahasia pada Vigenere Cipher Menggunakan Kombinasi Caesar Cipher dan Multiple-Key," JIMP-J. Inform. Merdeka Pasuruan, vol. 8, no. 1, pp. 28-31, 2023.