Implementation of novel cryptographic technique for enhancing the cipher security for Resilient Infrastructure

Fadhel K. Jabor[1], Noora zidan khalaf [2], Bourair Al-Attar[3,*], Hussein A. Hussein Al Naffakh[3] , J. F.Tawfeq [4]

[1] Vice President Office for Scientific Affairs, University of Baghdad, Baghdad, Iraq
[2] Quality Assurance & University Performance, Mustansiriyah University, Baghdad, Iraq
[3] College of Medicine, University of Al-Ameed, Karbala 1238, Iraq
[4] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad, Iraq
Emails: fadhel.k.jabor@uobaghdad.edu.iq; noora.zidan6@uomustansiriyah.edu.iq; bourair.alattar@alameed.edu.iq; aulanone@gmail.com; jamaltawfeq55@gmail.com
* Corresponding author's Email: bourair.alattar@alameed.edu.iq

Abstract

Cryptography is a well-known technology for providing confidential data transfer via asymmetric or symmetric algorithms with public or private keys. Secure data transmission over networks using unreliable, untrusted channels is made achievable by cryptography. As a result of the quick digital transition, network traffic is rapidly rising, and consumers remain constantly connected and accessible online. Extortions, including transforming, spoofing, and tracking data through unauthorised access, are quite widespread over the internet. Many more cryptographic algorithms already exist, but they need to be consistently improved and optimized for better performance within the constraints imposed by new technology and a wide variety of application domains. To overcome these limitations, we suggest a novel FishyCurve Cipher technique by combining an elliptic curve-based algorithm (ECA) with a Threefish cipher algorithm (TCA) to improve cipher security and performance, the data will be encrypted using TFCA, and the key will be secured by the EC technique. To verify data integrity, a digital signature algorithm (DSA) is employed. To evaluate the effectiveness of the proposed FishyCurve Cipher technique, comprehensive experimental tests have been conducted. The results clearly demonstrate its superiority in terms of cipher security when compared to traditional encryption algorithms. Its outstanding resilience against a wide range of attacks makes it a strong method of securing resilience infrastructure from malicious actors who seek to compromise data confidentiality and integrity.

Keywords: Encryption; Algorithm based on elliptic curves; A cryptographic algorithm based on threefish; Signing algorithm for digital documents; Security of ciphers; Innovation in processes; The resilience of infrastructure**.**

1. Introduction

As digital communication has grown and online platforms have become more widely used, the importance of secure data transmission has become critical. The cryptographic foundation ensures confidentiality, integrity, authentication, and non-repudiation as a critical technology [1]. Information can only be accessed and understood by authorized parties under confidentiality. Data integrity ensures that the data remains intact and unaltered during transmission and storage. To prevent impersonation or unauthorized access, authentication verifies communication parties' identities. Messages are non-repudiated if the sender cannot deny having sent them. To make plaintext information unintelligible to unauthorized individuals, cryptography uses mathematical algorithms and principles. This technology allows secure data transmission using public or private keys in combination with asymmetric or symmetric algorithms. Cryptography consists of symmetric/asymmetric key encryption and public key cryptography. Symmetric key encryption, sometimes referred to as secret key encryption, uses the same shared secret key for encryption and decryption. Data is encrypted and decrypted using the same key by both the sender and recipient. Two keys are mathematically linked with asymmetric key

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

encryption, also known as public key encryption [4]. There are two keys: a public and a private one. The public key is freely disseminated, whereas the private key is kept secret. Only the recipient with the right private key will be able to decrypt messages encrypted with the public key. Cryptographic techniques are not just about encryption; they also include hash functions and digital signatures. Data integrity is ensured by ensuring that no tampering has occurred with hash values generated from input data. Signatures provide non-repudiation and authentication by binding messages or documents to the identity of their authors through asymmetric key encryption [5]. Using strong ciphers, which convert plaintext into encrypted text, is one of the fundamental aspects of cryptographic security. Cryptographic attacks and advances in computing power require constant improvements in ciphers' security, even though they are designed to be secure. Securing algorithms requires rigorous implementation, proper key management practices, and secure algorithm design. To meet the ever-increasing demand for secure communication and data protection, cryptography will continue to evolve as new cryptographic attacks and computing technologies emerge [6]. In the past few years, network traffic has skyrocketed as the internet has become a more integral part of people's lives as advances in digital technology continue to transform our everyday lives. There are numerous threats that have arisen in this digital landscape, such as data tampering, impersonation, and unauthorized access. Cryptographic solutions are necessary to prevent these threats. A new generation of cryptographic algorithms is required to solve problems related to new threats and computational power to make ciphers more secure. With FishyCurve Cipher, we are addressing these challenges. To maximize the performance and security of ciphers, ECA and TCA are combined. By using a TCA, FishyCurve Cipher provides encryption and confidentiality for data. In conjunction with the encryption keys, the ECA provides an additional layer of security. Our goal is to provide a more robust and resilient data transmission solution using both algorithms. Moreover, FishyCurve Cipher incorporates digital signatures to make data integrity even better. According to the paper's structure, Part 1 briefly discusses cryptography and the challenges and threats of constant connectivity and digital transition in the data security industry. Particularly, part 2 discusses how ciphers can be enhanced to enhance the security and performance of data transmissions over networks. In part 3, we explain how to evaluate the proposed technique. In part 4, FishyCurve Cipher's performance is evaluated. The FishyCurve Cipher technique is highlighted in Part 5 to enhance the security and performance of ciphers.

2. Related Works

As specified in article [7], reducing calculations and responses can improve the security of Diffie-Hellman algorithms. A hash of all values being transmitted across a network was introduced as part of the modified Diffie-Hellman algorithm to make it more secure against attacks. Researchers have proposed an innovative symmetric key cryptographic solution inspired by DNA cryptography. The suggested system was based on a randomized, dynamic encoding table that would provide higher security. In the security analysis, a plaintext attack (CPA) was found to be secure against the suggested technique. It was demonstrated that the proposed encryption strategy is more effective than alternative symmetric key encryption techniques in the work by introducing a novel encryption method for secure data transfer. According to the proposed encryption strategy, FiGenère cipher is based on vector spaces of finite dimensions. In addition, the proposed method relies on key selection randomization as a decomposition, which could continue forever. To further complexity and produce the most chaotic result possible in the encrypted text structure, a peculiar substitution cipher key was added to the "text scrambling process". An efficient PRESENT cipher with fewer rounds of encryption, updated "Keys registers," and an additional layer between the "S-box and P-layer" in the encryption-decryption method was presented in a study [10]. The value of the key register is encrypted using the delta value function of TEA. With this extra protection, the PRESENT cycle just must be reduced to 25 rounds. The efficiency of the method is improved by "encrypting the key register". The integration of the "Arnold chaotic map (ACM) and Rivest Cipher 4 (RC4)" was used in the research [11] to suggest a cryptography approach in a medical image. ACM was a chaotic cryptographic method that outperformed brute force and deference assault. The purpose of "chaotic cryptography" was to muddle the pixel position. In comparison, the stream cipher method RC4 was immune to computational and statistical fasts. These two algorithms would be combined to produce better encryption methods that perform well and can be performed rapidly.

The "Asymmetric Key Blum-Goldwasser Cryptography (AKBGC)" method was suggested in the article [12] to improve cloud service security for communication. Blum-Goldwasser Cryptography (BGC) was used by the cloud server to deliver the services it requires to customers in the cloud while maintaining better levels of secrecy and data security. During the transfer, the user-required cloud information was encrypted using the "probabilistic encryption algorithm" provided by BGC and the public key of the intended receiver using the AKBGC method. To access original cloud data, the AKBGC method authenticates keys at the receiver. When the sender and receiver public keys are the same, BGC's deterministic decryption algorithm can reconstitute the original data. It enhances cloud service provisioning communication security for the AKBGC method.In the article [13], the “two most significant ciphers, Polybius and Vigenère,"are combined to create a novel hybrid

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

security cipher. In comparison, this hybrid encryption cipher offered more security than traditional ciphers.In the study [14], they investigate a two-level serialization-based ultra-lightweight RC5 block cipher implementation. The "data-dependent rotation (DDR)" module, which was part of the RC5 block cipher that requires the most processing power, was also optimized via a resource-sharing method.Two different cryptographic techniques are used in the encoding process of the study [15]. There are two types of algorithms: one is the Vigenere Cipher algorithm, and the other is the RSA (Rivest Shamir Adleman) algorithm. The mathematical analysis reveals that the encryption was more secure than before due to the employment of two encodings: one for the messages using the Vigenere Cipher cryptographic algorithm and another for the keys using the RSA algorithm. In the research [16], they suggest strengthening the TTIE algorithm with an additional layer of security and demonstrating how the TTIE-generated encryption key can be securely transferred to the other party using the Diffie-Hellman method. This study, therefore, presents and examines a variant of TTIE, the "Diffie Hellman Text-to-Image Encryption method (DHTTIE)."

In the study [17], they propose a security architecture for cloud computing that utilizes many layers of cryptography. The security of cloud storage was improved using the Data Encryption Standard (DES) and RSA, which allow for many layers of encryption and decryption at both ends of the communication. To lessen security risks, the paradigm provides clarity for both cloud users and providers. Compared to the current system, the model significantly improves data security and speeds up the uploading and downloading of texts.

A study [18] created a method to increase the security of the Vigenere cipher using "Rivest-Shamir-Adleman (RSA)."Public and private keys are used in the asymmetric algorithm RSA. The difficulty in identifying factors for the huge composite numbers was an advantage of employing the technique. The process took a lot of time but was secure. To make the proposed algorithm secure and faster than the RSA algorithm, they merged RSA with the Vigenere cipher in this technique. The method was frequently employed to encrypt SMS.
In the article [19], a unique, lightweight homomorphic cryptographic technique with two levels of encryption was presented. To improve data security in cloud computing, a new effective, "lightweight cryptographic technique" was utilized in the initial layer, while additive "homomorphic algorithms" were investigated in the following layer. The technique provides properties of both symmetric and asymmetric cryptography. The experimental outcomes of the proposed method showed a high level of security.

A study [20] presented a "hybrid proxy re-encryption technique" that uses "lightweight symmetric and asymmetric encryption algorithms" to protect fog-to-things computing interactions. Fog nodes' re-encryption computations are efficient in the proposed approach. For resource-constrained users, the approach reduces encryption and decryption overheads. Our approach was secure, efficient, and lightweight after security and performance evaluations. Security challenges and vulnerabilities have increased because of the rapid growth of digital communication and the growing reliance on network-based data transmission. The security and performance of current cryptography methods are both constrained. Assuring secure and confidential data transfer through networks while using inconsistent and unreliable methods has become a challenge. The risk of data alterations, spoofing, and unwanted access is exacerbated by high network traffic and users' continual connectivity. Despite being widely used, traditional encryption methods may not offer enough resistance against different attacks. A novel FishyCurve Cipher technique that addresses these restrictions and improves cipher security [21-27].

3. Methods

The suggested approach, which employs several cryptographic-based data security techniques, is an effective method. The approach uses more accurate digital signatures with an MD52 hashing method together with symmetric and asymmetric encryption to guarantee data integrity. The encryption speed of the algorithm needs to be taken into consideration, in addition to the compromise among speed and performance. Public key asymmetric key generation methods require greater generation time than symmetric, asymmetric key generation techniques. As a result, with this approach, the data is encrypted using a TCA. An overview of the solution is shown in Fig.1.

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

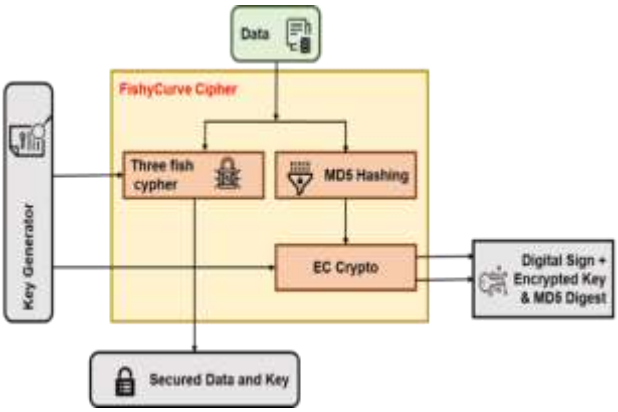

Figure 1: Outline of the suggested methodology

The initial data will first be hashed using MD5, which will be employed to verify the accuracy of the data. The second stage will include creating digital signatures using the EC technique and protecting the MD5 code and private key. The execution time of the EC can be reduced if we maintain a high level of security while maintaining the key and hash code minimal. Finally, a symmetric method called a TCA that has minimal encryption/decryption time will be used to encrypt the original material. Each stage of the solution is thoroughly explained in the sections that follow.

3.1 Digital signature

To ensure the authenticity of the data, this research employed a combination of digital signatures and hashing. Because the traditional paradigm of digital signatures is extremely susceptible to attacks, this method hashes the message and then signs the hash. Using a digital signature's authentication procedure, a hacker can create an unauthorized digital signature. The attacker cannot modify or damage the message's content since the digital signature does not match the message's hashing. Consequently, implementing a digital signature may be considered an effective approach for protection. The suggested solution's workflow for employing a hash code and digital signature is shown in Fig. 2.

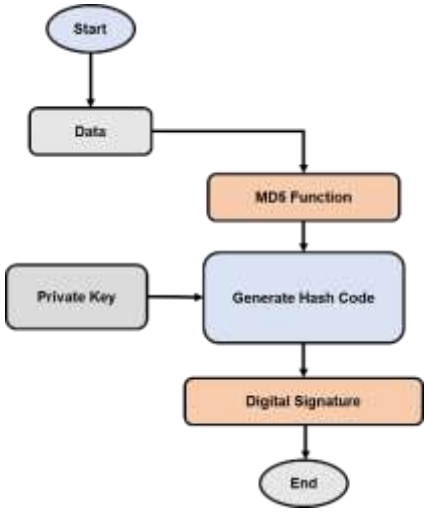

Figure 2: Flowchart for a digital signature and hash code.

3.2 ata encryption

The Three Fish cipher algorithm, which is both secure and easy to implement, uses multiple rounds of computing that are each increasingly simplified. The fundamental concept of Three Fish is the idea that "more simple rounds are more reliable than lesser complicated iterations."The only three operations used by Three Fish are left-bit rotation, bitwise exclusive OR, and addition modulo2^64. Three Fish only works on unregistered 64-bit integers. To create 64-bit words, the plain text Q and the encryption key L are transformed.

3.3 Key scheduling

The block cipher key$L = (l_0, l_1, l_2, l_3, \ldots, l_{NW-1})$ and 128-bit data $S = (s_1, s_2)$ are used to create the subkeys via the key schedule. K and T are expanded with a single integrity word. Each subkey consists of two words from the prolonged data, two words from the extended key, and a counter for each. Observe that the protracted

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

key and data have been changed by a one-word position over two successive sub-keys. Pseudocode 1 shows the process of key scheduling in the Three Fish cipher Algorithm. Note: Input as IN and output as OP.

Pseudocode 1. Process of key scheduling

IN: A block cipher key l, a data value S, a constant Value $C_{240} = IBD11BDAA9FC1A22.$
OP: $N_r/4 + 1$ *subkeys,* $l_{s,0}, l_{s,1}, \ldots, l_{s,Nw-1}$, *where* $0 \leq t$

$L_{Nw} \leftarrow C_{240} \oplus (l_0 \oplus l_1 \oplus \ldots \oplus l_{Nw-1})$
$s_2 \leftarrow s_0 \oplus s_1.$
For $t \leftarrow 0$ *to* $N_r/4$ *do*
    For $j \leftarrow o$ *to* $N_w - 4$ *do*
$l_{t,j} \leftarrow l_{(t+j)\,mod\,(Nw+1)};$
end for
$l_{s,Nw-3} \leftarrow l_{(s+Nw-3)\,mod\,(Nw+1)} \boxplus s_{t\ mod\ 3};$
$l_{s,Nw-2} \leftarrow l_{(s+Nw-2)\,mod\,(Nw+1)} \boxplus s_{(t+1)\ mod\ 3};$
$l_{s,Nw-1} \leftarrow l_{(s+Nw-1)mod(Nw+1)} \boxplus S_{t;}$
end for
return $l_{t,0}, l_{t,1,\ldots\ldots,l_{s,Nw-1,}}$
    Where $0 \leq t \leq N_r/4;$

3.4 A Block Diagram for TCA

The encryption structure is as follows: l is the key, s is the input, and q is the plain text, each of which is 32 bits long. l is also key, s is the input, and q is the plain text, which has been generated as 128-bit positions in the modified buffer, which has been used to generate 256-bit output keys as input to the key scheduler. The key scheduler generates 18 keys and operates based on the algorithm one randomly generated values. As illustrated in the internal block diagram that follows in Fig. 3, we can encrypt text using any one of these keys.

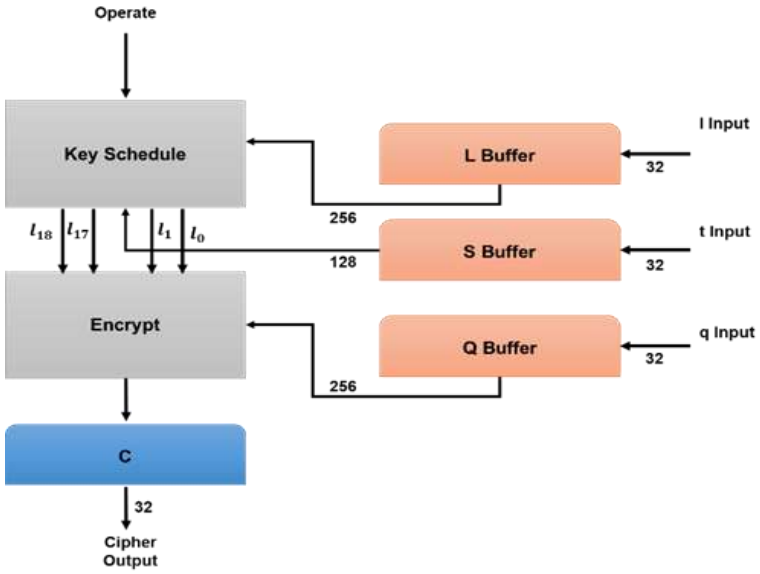

Figure 3: Block diagram for TFA

One of the 32 encryption block iterations is Fig. 4. Where v stands for positional velocity, and the encrypted sub key is produced as demonstrated by the modulo additions process. The algorithm2 below illustrates how the generated values are combined with the combining block and created random values. The obtained keys will probably be permuted using the below-described algorithm 2's vital conditions.

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

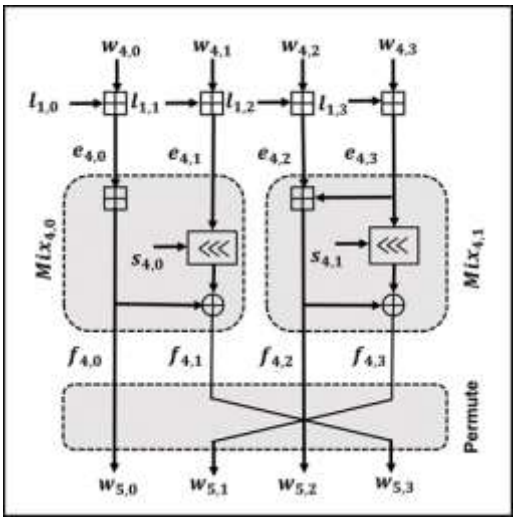

Figure 4: Representation of standard encryption

3.5 Encryption

The algorithm for the three-fish encryption standard is displayed below. The encryption block diagram is as follows: l is the key, S is the input, and q is the plain text. l is the key, s is the modified input, and q is the plain text, each of which is 32 bits long. l is also key, s is the input, and S is the buffer, which has generated the 128-bit positions for each of S1, S2, and plain text as data to the key scheduler. With the aid of any one of the 18 keys that the key scheduler generates, we may encrypt text using encryption algorithm 2 by using the key scheduler to operate depending on the randomly produced values as demonstrated in algorithm 1. Where w stands for positional velocity, and the encrypted sub key is created using the modulo addition method, as indicated. As illustrated below, Algorithm 2 combines the created random values with the generated values that were multiplied by the same amount of the generated values. The keys generated by Pseudocode 2 below are probably permuted with the required condition.

Pseudocode 2: Process of encryption using TCA

IN:

- *A plaintext block* $Q = (q_0, q_1, \dots\dots, qN_w - 1)$ *of size* N_w.
- $N_r/4 + 1$ *subkeys,* $k_{s,0}, k_{s,1}, \dots . k_{s,N_w-1}$, *where* $0 \le s \le N_r/4$.
- $4N_w$ *rotation constants* R_j, k, *where* $0 \le j \le 7$ *and* $0 \le k \le N_w/2$.

OP:

A cipher block$C = (c_0, c_1, \dots, c_{N_w-1})$.

Initialize intermediate state array $w_{0,j}$ *with values from the plaintext block Q:* $w_{0,j} \leftarrow q_j$.

Iterate over the number of rounds (d) from 0 to $N_r - 1$*: a. Iterate over the intermediate state array indices (j) from 0 to* $N_v - 1$*:*

- *If* $d \bmod 4 = 0$, *perform key injection:* $e_{d,j} \leftarrow w_{d,j} \boxplus k_{d/4,i}$.
- *Otherwise, perform renaming:* $e_{d,j} \leftarrow w_{d,j}$.

Iterate over the indices (k) from 0 to $N_w/2 - 1$*:*

Perform XOR and rotation operations:

$f_{d,2k} \leftarrow e_{d,2k} \boxplus e_{d,2k+1}$.

$f_{d,2k+1} \leftarrow f_{d,2k} \oplus (e_{d,2k+1} \lll R_{d \bmod 8,k})$.

Iterate over the intermediate state array indices (k) from 0 to $N_w - 1$*:*

Apply permutation: $v_{d+1,j} \leftarrow f_{d,\pi(j)}$.

Iterate over the indices (k) from 0 to $N_w - 1$*:*

Perform key injection on the output block:$c_k \leftarrow v_{N_r,j} \boxplus k_{N_r/4,j}$.

Return the cipher block $C = (c_0, c_1, \dots . , c_{N_w-1})$

To create the ciphertext, N_r rounds are done continually, and then the final subkey addition is carried out. The fundamental nonlinear mixing function is the basis of a round. It is composed of an addition, a rotation by the value of $R_{d,k}$ (specified in Table 2 and repeated every eight rounds), and a bitwise exclusive OR. The result of the round is then obtained by applying a word permutation $\pi(j)$ in Table I. A subkey is additionally introduced every four rounds.

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

Table 1: Value Of $\pi(j)$

j	0	1	2	3
$\pi(j)$	0	3	2	1

Table 2. Outcome Of $R_{d,j}$

d	0	1	2	3	4	5	6	7
$j=0$	14	52	23	5	25	46	58	32
$j=1$	16	57	40	37	33	12	22	32

3.6 Decryption

Three Fish 256 decryption round. It starts with the inverse word permutations and then continues to the inverse MIX functions. Notice that the subkeys are inserted in the reverse order. One of the 72 iterations of decryption is depicted in Figure 5. The block diagram for decryption is as follows. Ciphered text is most likely permuted with the essential conditions in method two described above where L keys S is the inputs and C is the cipher text each of 32 bits where w denotes position velocities and decrypted sub key is formed by modulus subtraction operation as indicated. The created values again modulo extra and is inverted mixed with the mixing block generating random values, as illustrated below in Fig. 5.

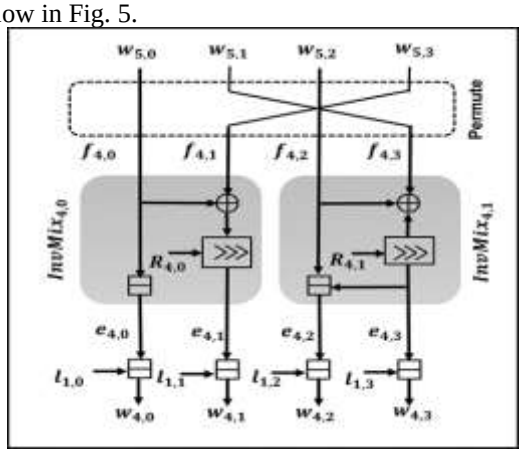

Figure 5: Representation of standard decryption

3.7 Security of the symmetric-Key

For methods that use symmetric keys, like TCA, giving out the secret key could be risky because attackers might obtain the key. EC-based cryptography, that is, an asymmetric technique, is used to protect the "private key and hash function" in this method. To outperform existing approaches, this technique will employ a 164-bit key. EC-based encryption methods provide a high level of protection and use minimal store space and bandwidth. This encryption is useful because it can be used across limited fields. High levels of protection are offered by EC-based encryption techniques, which also consume less bandwidth and more storage space. This encryption is advantageous since it may be used in a few different fields.

The Elliptic curve EC is identical to the equation if$q > 3$ is an odd prime, and $b, \in Fq$ and $4b^3 + 27c^2 \neq 0$ mod q.

$$z^2 = y^3 + by + c \quad (1)$$

Using Q, which can build a unit in $E(Fq)$, and taking into account $p = (x1, y1)\ \{p, Q\}\ \in E(Fq)$

For point adding $Q + R = (y_3, z_3)$ and $Q \pm R$

$$y_3 = \lambda^2 - y_1 - y_2 \quad (2)$$

$$z_3 = \lambda(y_1 - y_3) - z_1 \quad (3)$$

$$\lambda = (z_2 - z_1)/(y_2 - y_1) \quad (4)$$

For point doubling $Q + Q = 2Q(y_3, z_3)$

$$y_3 = \lambda^2 - 2y_1 \quad (5)$$

$$z_3 = \lambda(y_1 - y_3) - z_1 \quad (6)$$

$$\lambda = (3y_1^2 + b)/2z1 \quad (7)$$

We initially select a random k integer from a field-appropriate range and treat it as the "private key" for EC cryptography. Then, using $R = kQ$, the "public key R" will be determined. Q is an EC point in this case. EC encryption reduces the computational effort when computing k from Q and R points. The complexity of the discrete logarithm issue affects EC encryption. This method makes use of the ensuing scalar multiplication.

$$r = k.Q = Q + Q + \cdots + Q \quad (8)$$

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

The efficiency of elliptic-curve cryptography can be enhanced by utilizing Modular Multiplication since the processes in this approach are based on the field. The process is outlined in the next several phases.

i. The data to be encrypted will first have a hash code (created with MD5) produced. This code's purpose is to improve the data integrity verification and digital signature and procedures more efficiently.
ii. After the hash code has been encrypted using the "private key," a digital signature for the data will be created.
iii. EC cryptography will be used to encrypt the Threefish private key.
iv. Threefish, a symmetric encryption technique, will be used to encrypt the information. Using the symmetric key, the initial data is encrypted. The transmitted data that is encrypted from this step and the ones before it will finally be decoded.
v. The receiver employs a reversible method and the private key to decrypt the transmitted data.
vi. The hash function (digital signature) will be used for validation and verification once the original data has been decrypted with the threefish private key.

4. Results and Discussion

This section primarily focuses on the effectiveness of the suggested FishyCurve for enhancing security in cipher. The performance of the hybrid symmetric and asymmetric encryption to secure the cipher from hackers was discussed in this part. The existing methods are ERSA [21], ESKEA [22], and HE+BE [23]. The parameters are encryption time, decryption time, key generation time, CPU utilization, throughput (Mbps), and security level. To analyze the approach's performance with tiny data, we first evaluated it by 50 KB, 100 KB, 150 KB, 200 KB, and 250 KB. Encryption Time refers to the duration it takes to transform a plaintext message or data into ciphertext using a specific encryption algorithm. It measures the time required for the encryption algorithm to process the input data and apply cryptographic operations to convert it into an unreadable and secure format. Fig. 6 depicts the encryption time result, and Table III indicates the values of encryption time. Comparing the suggested cryptographic algorithm (FishyCurve) with the current cryptographic algorithm (ERSA, ESKEA, and HE+BE), our FishyCurve takes less time to encrypt the data. This cryptographic algorithm performs effectively when compared to the alternative strategy.

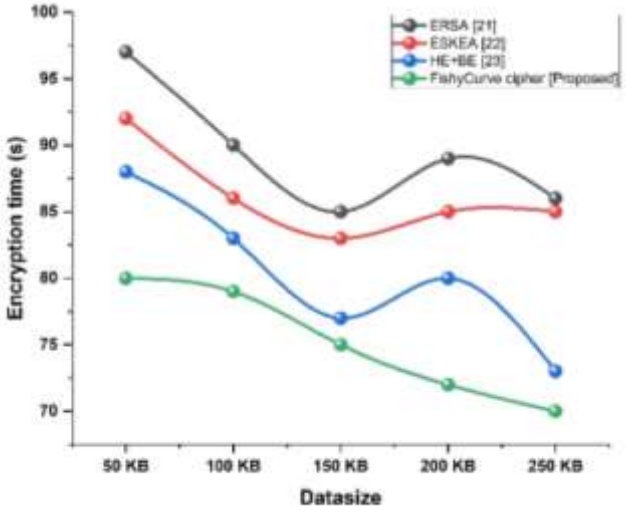

Figure 6: Encryption result

Table 2: Value Of Encryption Result

Data size	**Encryption time (s)**			
	ERSA [21]	ESKEA [22]	HE+BE [23]	FishyCurve cipher [Proposed]
50	97	92	88	80
100	90	86	83	79
150	85	83	77	75
200	89	85	80	72
250	86	85	73	70

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

It represents the time taken to decrypt the ciphertext back into its original plaintext using the decryption algorithm. It measures the processing time required to revert the encrypted data to its original form. Fig. 6 depicts the decryption time result, and Table IV indicates the values of decryption time. Comparing the suggested approach (FishyCurve) with the current methods (ERSA, ESKEA, and HE+BE), it is clear that our cryptographic algorithm takes less time to decrypt the data. This cryptographic algorithm performs superior to the other cryptographic methods.

Figure 7: Decryption result

Table 3: Value Of Decryption Result

Data size	**Decryption time (s)**			
	ERSA [21]	ESKEA [22]	HE+BE [23]	FishyCurve cipher [Proposed]
50	97	93	91	89
100	94	90	89	83
150	91	89	86	80
200	92	89	83	75
250	90	87	85	70

Key generation time refers to the time required to generate a cryptographic key for encryption and decryption purposes. This process involves generating a random or pseudo-random key that satisfies the requirements of the encryption algorithm. The results of the key generation time are depicted in Fig. 8, and the key generation time values are shown in Table V. By contrasting the recommended cryptographic algorithm (FishyCurve) with the existing cryptographic algorithm (ERSA, ESKEA, and HE+BE), it is evident that our suggested methodology requires the least amount of time for key generation. Compared to other cryptographic key generation techniques, our FishyCurve cryptographic is more effective.

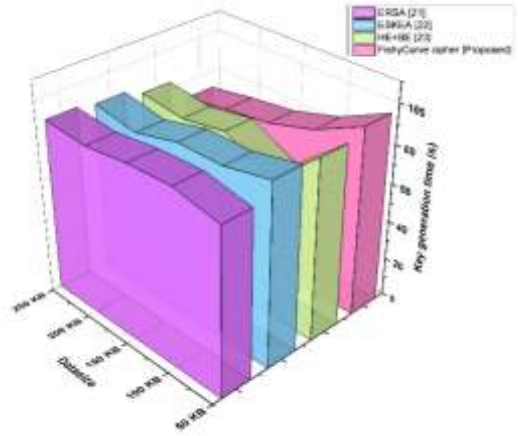

Figure 8: Outcome of key generation time

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

Table 4: Result Value of Key Generation Time

Data size	Key generation time (s)			
	ERSA [21]	ESKEA [22]	HE+BE [23]	FishyCurve cipher [Proposed]
50	86	94	93	97
100	91	89	72	85
150	90	89	84	78
200	87	83	80	75
250	89	87	83	71

CPU utilization refers to the percentage of time that the CPU is actively executing tasks compared to the total available CPU time. A CPU utilization graph visually represents the variations in CPU usage over a specific period. Fig. 9 displays the CPU utilization results, and Table VI displays the CPU utilization result value. A lower line on the graph, when compared to the previous cryptographic technique, illustrates how efficient the cryptographic algorithm is in terms of CPU utilization. Compared to our cryptography approach, our FishyCurve algorithm is more efficient.

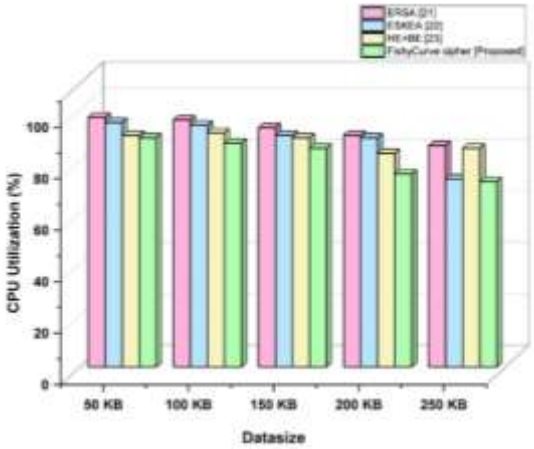

Figure 9: Outcome of CPU utilization

Table 5: Result Value of Cpu Utilization

Data size	CPU Utilization (%)			
	ERSA [21]	ESKEA [22]	HE+BE [23]	FishyCurve cipher [Proposed]
50	97	95	90	89
100	96	94	91	87
150	93	90	89	85
200	90	89	83	75
250	86	73	85	72

Throughput refers to the amount of tasks completed or data processed per unit of time. In the context of a graph, a throughput graph represents the rate at which data is processed or a task is completed over time. The throughput data are depicted in Figure 10, and the throughput value is shown in Table 7. By contrasting the recommended cryptographic algorithm (FishyCurve) with the existing cryptographic algorithm (ERSA, ESKEA, and HE+BE), it is evident that our suggested cryptographic algorithm requires high throughput. The Our FishyCurve algorithm is more effective than our cryptography strategy.

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

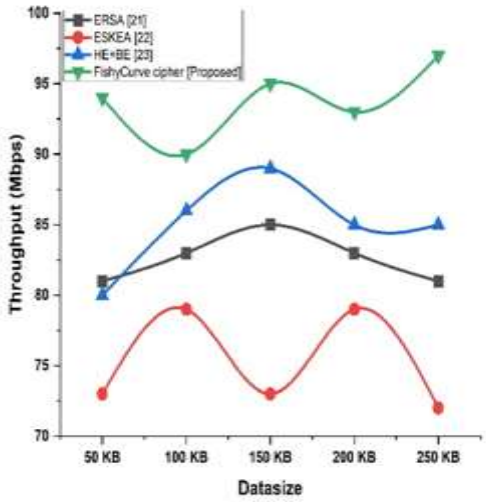

Figure 10: Outcome of Throughput

Table 6: Result Value of The Throughput

Data size	Throughput (Mbps)			
	ERSA [21]	ESKEA [22]	HE+BE [23]	FishyCurve cipher [Proposed]
50	81	73	80	94
100	83	79	83	90
150	85	73	89	95
200	83	79	85	93
250	81	72	85	97

5. Conclusion

Cryptography is a very important part of making sure that data transfers over networks are safe. The importance of secure and dependable communication has increased with the prevalence of digital technology and continuous connectivity. There are several ways to convey sensitive data, including using symmetric and asymmetric cryptographic techniques that employ public and private keys. By encrypting the key via EC asymmetric cryptography, symmetric key exchange concerns, including key theft in transit, are eliminated. In addition to its benefits, the method uses MD5-based digital signatures to ensure data integrity. In comparison to ERSA, ESKEA, and HE+BE, the cryptographic algorithm assessment reveals a general improvement. The results clearly demonstrate its superiority in terms of cipher security when compared to traditional encryption algorithms. The FishyCurve Cipher technique exhibits remarkable resilience against a wide range of attacks, providing a robust defense against malicious actors seeking to compromise data confidentiality and integrity. The FishyCurve Cipher approach uses the elliptic curve-based algorithm for safe key management, although key creation, distribution, and storage is still crucial to any cryptographic system. Key derivation and hardware security modules can be explored in future key management research.

References

[1] Gawer, “Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age,” Innovation, vol. 24, no. 1, pp. 110–124, Sep. 2021, doi: 10.1080/14479338.2021.1965888.

[2] Pan, N. Stakhanova, and S. Ray, “Data provenance in security and privacy,” ACM Computing Surveys, Apr. 2023, doi: 10.1145/3593294.

[3] Ioniță, “Weighted Attribute-based Encryption with Parallelized Decryption,” Proceedings of the 19th International Conference on Security and Cryptography, 2022, doi: 10.5220/0011278400003283.

[4] K. R. Raghunandan, A. Ganesh, S. Surendra, and K. Bhavya, “Key Generation Using Generalized Pell’s Equation in Public Key Cryptography Based on the Prime Fake Modulus Principle to Image Encryption and Its Security Analysis,” Cybernetics and Information Technologies, vol. 20, no. 3, pp. 86–101, Sep. 2020, doi: 10.2478/cait-2020-0030.

[5] P. K. Shukla, A. Aljaedi, P. K. Pareek, A. R. Alharbi, and S. S. Jamal, “AES Based White Box Cryptography in Digital Signature Verification,” Sensors, vol. 22, no. 23, p. 9444, Dec. 2022, doi: 10.3390/s22239444.

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

[6] N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," Sensors, vol. 22, no. 9, p. 3520, May 2022, doi: 10.3390/s22093520.
[7] S. Ali et al., "An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 16, no. 6, p. 155014772092577, Jun. 2020, doi: 10.1177/1550147720925772.
[8] M. Sohal and S. Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 1, pp. 1417–1425, Jan. 2022, doi: 10.1016/j.jksuci.2018.09.024.
[9] N. Uniyal, G. Dobhal, A. Rawat, and A. Sikander, "A Novel Encryption Approach Based on Vigenère Cipher for Secure Data Communication," Wireless Personal Communications, Mar. 2021, doi: 10.1007/s11277-021-08295-5.
[10] R. Chatterjee and R. Chakraborty, "A Modified Lightweight PRESENT Cipher For IoT Security," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Mar. 2020, doi: 10.1109/iccsea49143.2020.9132950.
[11] Irawan, D. R. I. Moses Setiadi, E. H. Rachmawanto, C. A. Sari, and M. Doheir, "Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security," Journal of Physics: Conference Series, vol. 1201, no. 1, p. 012022, May 2019, doi: 10.1088/1742-6596/1201/1/012022.
[12] Boneh, "Blum–Goldwasser Public Key Encryption System," Encyclopedia of Cryptography and Security, pp. 51–52, doi: 10.1007/0-387-23483-7_38.
[13] S. Vatshayan, R. A. Haidri, and J. Kumar Verma, "Design of Hybrid Cryptography System based on Vigenère Cipher and Polybius Cipher," 2020 International Conference on Computational Performance Evaluation (ComPE), Jul. 2020, doi: 10.1109/compe49325.2020.9199997.
[14] Y. A. Birgani, S. Timarchi, and A. Khalid, "Ultra-lightweight FPGA-based RC5 designs via data-dependent rotation block optimization," Microprocessors and Microsystems, vol. 93, p. 104588, Sep. 2022, doi: 10.1016/j.micpro.2022.104588.
[15] "Hybrid Cryptosystem Analysis by Using The Combination of Vigenere Cipher and RSA for Text Security," Proceeding on International Conference of Science Management Art Research Technology, Oct. 2020, doi: 10.31098/ic-smart.v1i1.31.
[16] Abusukhon, M. N. Anwar, Z. Mohammad, and B. Alghannam, "A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm," Journal of Discrete Mathematical Sciences and Cryptography, vol. 22, no. 1, pp. 65–81, Jan. 2019, doi: 10.1080/09720529.2019.1569821.
[17] S. Kumar, G. Karnani, M. S. Gaur, and A. Mishra, "Cloud Security using Hybrid Cryptography Algorithms," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), Apr. 2021, doi: 10.1109/iciem51511.2021.9445377.
[18] B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," Journal of the Operations Research Society of China, vol. 10, no. 4, pp. 835–848, Aug. 2020, doi: 10.1007/s40305-020-00320-x.
[19] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing," International Journal of Intelligent Networks, vol. 3, pp. 16–30, 2022, doi: 10.1016/j.ijin.2022.04.001.
[20] O. A. Khashan, "Hybrid Lightweight Proxy Re-Encryption Scheme for Secure Fog-to-Things Environment," IEEE Access, vol. 8, pp. 66878–66887, 2020, doi: 10.1109/access.2020.2984317.
[21] R. Nidhya, S. Shanthi, and M. Kumar, "A Novel Encryption Design for Wireless Body Area Network in Remote Healthcare System Using Enhanced RSA Algorithm," Intelligent System Design, pp. 255–263, Aug. 2020, doi: 10.1007/978-981-15-5400-1_27.
[22] S. Elkana Ebinazer, N. Savarimuthu, and S. Mary Saira Bhanu, "ESKEA: Enhanced Symmetric Key Encryption Algorithm Based Secure Data Storage in Cloud Networks with Data Deduplication," Wireless Personal Communications, vol. 117, no. 4, pp. 3309–3325, Nov. 2020, doi: 10.1007/s11277-020-07989-6.
[23] K. R. Sajay, S. S. Babu, and Y. Vijayalakshmi, "Enhancing the security of cloud data using hybrid encryption algorithm," Journal of Ambient Intelligence and Humanized Computing, Jul. 2019, doi: 10.1007/s12652-019-01403-1.
[24] G.O. Ogunleye, & Akinsanya, S. . (2022). Elliptic Curve Cryptography Performance Evaluation for Securing Multi-Factor Systems in a Cloud Computing Environment. Iraqi Journal of Science, 63(7), 3212–3224. https://doi.org/10.24996/ijs.2022.63.7.40.
[25] Khodher, M. A. A., Alabaichi, A., & Altameemi, A. A. (2022). Steganography Encryption Secret Message in Video Raster Using DNA and Chaotic Map. Iraqi Journal of Science, 63(12), 5534–5548. https://doi.org/10.24996/ijs.2022.63.12.38.
[26] Jawad, R. N. (2022). Proposed Hybrid Technique in Cryptanalysis of Cryptosystem Based on PSO and SA. Iraqi Journal of Science, 63(10), 4547–4558. https://doi.org/10.24996/ijs.2022.63.10.37.

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024

[27] M. S. Jabbar, I. I. Al_Barazanchi, A. L. Khalaf, P. S. JosephNg, and A. D. Radhi, "Optimizing multi-antenna M-MIMO DM communication systems with advanced linearization techniques for RF front-end nonlinearity compensation in a comprehensive design and performance evaluation study," Period. Eng. Nat. Sci., vol. 11, no. 3, pp. 124–138, 2023, doi: 10.21533/pen.v11i3.3609.g1296.
[28] Y. Niu, I. A. M. Al Sayed, A. R. Ali, I. Al Barazanchi, and P. S. Josephng, "Research on fault adaptive fault tolerant control of distributed wind solar hybrid generator," Bull. Electr. Eng. Informatics, vol. 12, no. 2, pp. 1029–1040, 2023, doi: 10.11591/eei.v12i2.4242.

Doi: https://doi.org/10.54216/FPA.150103
Received: July 24, 2023 Revised: November 18, 2023 Accepted: February 09, 2024