http://www.doi.org/10.62341/rahl1379

Received	2026/02/18	تم استلام الورقة العلمية في
Accepted	2026/03/01	تم قبول الورقة العلمية في
Published	2026/03/02	تم نشر الورقة العلمية في

A Novel Hybrid Cryptographic Algorithm Based on SOA and Elliptic Curve Cryptography (ECC)

***Reem S. Fadeel [1], **Aml A. Altirban [1] and Hana H. Elgaramali [1]**

[1] Department of Mathematics, Faculty of Science, University of Tripoli, Libya

*r.fadeel@uot.edu.ly

**ORCID No 0009-0007-7183-9291

Abstract:

Protecting data confidentiality and integrity paramount in the digital ago. While symmetric encryption algorithms are fast, they struggle with secure key exchange, and asymmetric methods, though secure demand high computational resources. This gap necessitates a balanced cryptographic solution. This research introduces a novel hybrid encryption algorithm that merges the lightweight block-based structure of the SOA algorithm with the strong security features of Elliptic Curve Cryptography (ECC). The proposed method starts by dividing the plaintext into fixed-size blocks, converting characters int ASCII values, and applying alternating arithmetic operations-addition for odd-indexed blocks and subtraction for even-indexed blocks using fixed encryption matrices and a key complexity. In the decryption stage, the process is reversed using the ECC private key, the identity matrix, and a fixed matrix to reconstruct the text. By integrating ECC into the SOA structure, the need for insecure secret key exchange is eliminated, effectively transforming SOA into an asymmetric encryption system. The results demonstrate that the proposed hybrid approach achieves a strong balance between computational efficiency and high security making it suitable for resource constrained environments and secure data transmission.

Keywords: Elliptic Curve Cryptography (ECC), SOA Algorithm, Hybrid Cryptographic Algorithm, Compute initial key, private and public key.

خوارزمية تشفير هجينة جديدة تعتمد على تشفير SOA وتشفير منحنى البيضاوي (ECC)

ريم السنوسي فضيل [1*]، أمل عبد الله الطربان [1]، هناء حسن القره مانلي [1]

[1] قسم الرياضيات، كلية العلوم، جامعة طرابلس، ليبيا.

الملخص

حماية سرية البيانات وسلامتها أمران أساسيات في العصر الرقمي. بينما خوارزميات التشفير المتماثل سريعة، إلا أنها تواجه صعوبة في تبادل المفاتيح الآمن والطرق غير المتماثلة، رغم أن الأمان يتطلب موارد حسابية عالية. هذه الفجوة تتطلب حلا تشفيريا متوازنا. يقدم هذا البحث خوارزمية تشفير هجينة مبتكرة تدمج البنية الخفيفة البنية القائمة على الكتل لخوارزمية SOA مع ميزات الأمان القوية لتشفير المنحنى البيضاوي (ECC). تبدأ الطريقة المقترحة بتقسيم النص الواضح إلى كتل ذات حجم ثابت، وتحويل الأحرف إلى قيم ASCII، وتطبيق العمليات الحسابية المتناوبة – جمع الكتل الفردية المفهرسة والطرح للكتل ذات الفهرسة الزوجية باستخدام مصفوفات تشفير ثابتة وتعقيد مفتاح. في مرحلة فك التشفير، يتم عكس العملية باستخدام مفتاح ECC الخاص، ومصفوفة الهوية، ومصفوفة ثابتة لإعادة بناء النص. من خلال دمج ECC في هيكل SOA، يتم القضاء على الحاجة إلى تبادل المفاتيح السرية غير الآمنة، مما يحول SOA فعليا إلى نظام تشفير غير متماثل. تظهر النتائج أن النهج الهجين المقترح يحقق توازنا قويا بين الكفاءة الحاسوبية والأمان العالي، مما يجعله مناسبا للبيئات المحدودة للموارد ونقل البيانات الآمن.

الكلمات المفتاحية: تشفير المنحنى البيضاوي (ECC)، خوارزمية SOA، خوارزمية التشفير الهجينة، حساب المفتاح الابتدائي، المفتاح الخاص والعام.

1. Introduction

Security is a fundamental aspect of internet and network applications, which are expanding rapidly in today’s world. As the transmission and exchange of information over the internet and other communication channels continue to grow in scale and importance, ensuring the protection of this data has become

http://www.doi.org/10.62341/rahl1379

essential. Among the various approaches to safeguarding information, cryptography remains one of the most effective methods for securing data during transmission.

Based on the distribution of the key, encryption is classified into two main types symmetric key encryption and asymmetric key encryption (Mohammed Abdulhameed AL-Shabi,. 2019). In Symmetric encryption uses the same key for encryption and decryption while this method is simple and fast it presents a significant security challenge secure key exchange. Numerous studies have explored the strengths and weaknesses of symmetric algorithms, such as AES and DES, particularly in terms of speed and vulnerabilities during key distribution (Mohammed N. Alenezi, et al,. 2020, Ayushi, et al,. 2010). On the other hand, asymmetric encryption uses two separate keys a public key and a private key for decryption. Although it is more secure it tends to be slower in performance. Recent research in public key cryptography especially RSA and ECC, continues to improve key length and computational efficiency to meet practical requirements (Annapoorna Shetty; et al,. 2014, Xiangyu Chang, et al., 2022).

Among symmetric encryption methods, the SOA algorithm has been proposed as a lightweight block-based encryption technique (Samyrah Abu Irzayzah, et al., 2025). This algorithm works by dividing the plaintext into small blocks and generating a local key for each block based on its elements. Two fixed matrices (A and B), along with a random encryption key x, are used to encrypt the data. Characters are first converted into symbols using a unique mapping based on the number of blocks, which forms the numerical values used in the encryption process. An additional technique is applied during encryption by generating a key from the block numbers. This key adds another layer of confusion and enhances the overall encryption structure. However, the main limitation of the SOA structure is its reliance on the exchange of secret keys, which is risky in open communication environments.

In contrast, Elliptic Curve Cryptography (ECC) is one of the most powerful modern techniques in asymmetric encryption. It provides high security with shorter key lengths compared to other public-key systems such as RSA (Mohammad Rafeek Khan, et al. 2023). ECC has been extensively studied in cryptographic research for its ability to provide security equivalent to RSA but with much smaller key

http://www.doi.org/10.62341/rahl1379

sizes, making it ideal for constrained environments such as mobile and embedded systems (LARA-NINO, Carlos Andres Lara-nino, DIAZ-PEREZ, et al., 2018, Yuhan. Yan, 2022, ZHOU, Xin Zhou,. Xiaofei Tang,. 2011). It is based on digital signatures, and secure key exchange. One of its most significant advantages is strong security with lower computational cost.

In this research, we propose a hybrid encryption algorithm that combines the efficiency and simplicity of the SOA structure with the strong security of the ECC structure. The proposed system begins by dividing the plaintext into 2×1 blocks, converting characters into ASCII values, and applying alternating operations-addition for odd-indexed characters subtraction for even-indexed blocks along with fixed encryption matrices (A and B) and a key z generated by the ECC algorithm, followed by applying a pairing function to it (Arnold Rosenberg, 2003). For decryption, the process is reversed using the key z, the identity matrix, and a fixed matrix C. To overcome the key exchange issue in the SOA structure, ECC is integrated to generate asymmetric encryption system. This hybrid design aims to strike a balance between computational performance and high-level data security, building upon and extending previous research in both symmetric and asymmetric encryption.

2. Mathematical Preliminaries

Definition 2.1 [9]

A pairing function is a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$ that is also strictly monotone in each of its arguments.

$$P: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

Where $\mathbb{N}$ denotes the set of natural number.

An arbitrary pairing function can be denoted as $f(x, y)$, with pointed brackets $\langle x, y \rangle$ .If $\langle x, y \rangle$ is a pairing function, then it must allow recovery of each argument X and Y from $\langle x, y \rangle$. Hence, it is called as two function projection and it can be written as:

$$\pi_1\,(Z) = X \; and \; \pi_2\,(Z) = Y. \text{ If } \; Z = \langle x, y \rangle,$$
$$\text{Then, } \pi_1\,(Z) = X \; and \; \pi_2\,(Z) = Y.$$

http://www.doi.org/10.62341/rahl1379

Definition 2.2 [8]
An elliptic curve E over a prime field F_p is defied by

$$E{:}\, y^2 \equiv x^3 + ax + b \quad (\mathrm{mod}\, p) \tag{1}$$

Where $a, b \in \mathrm{F}_p,\ p \neq 2{,}3$ and satisfy the condition $4a^3 + 27b^2 \not\equiv 0\ (mod\ p)$. The elliptic curve group $E(\mathrm{F}_p)$ is the set of all points (x, y) that satisfy the elliptic curve Equation (1) beside a special point O at infinity.

2.1 Elliptic Curve Operations [10]

i. Point Addition.

Suppose $P = (x_1, y_1)\ and\ Q = (x_2, y_2)$, where $P \neq Q$, are two points lie on an elliptic curve E Equation (1). The sum $P + Q$ results a third point R which is also lies on E . To add two points on E there are some cases on the coordinates of the points P and Q . These cases are given as follows.

- If $P \neq Q \neq O$ with $x_1 \neq x_2$, then sum of $P\ and\ Q$ in this case is defined by

$$P + Q = R = (x_3, y_3). \tag{2}$$

Where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. (3)

$$x_3 = (\lambda^2 - x_1 - x_2)\ (\mathrm{mod}\, p) \tag{4}$$

$$x_3 = (\lambda(x_1 - x_3) - y_1)(\mathrm{mod}\, p) \tag{5}$$

- If $x_1 = x_2\ but\ y_1 \neq y_2\ then\ P + Q = 0.$

ii. Point Doubling.

Let $P = (x_1, y_1)$ be a point lies on E . Adding the point P to itself is called doubling point on an elliptic curve E . In other words

$$P + P = 2P = R = (x_3, y_3) \tag{6}$$

where

$$\lambda = \frac{3x_1^2 + a}{2x_1} \tag{7}$$

$$x_3 \equiv (\lambda^2 - 2x_1)(mod\ p) \tag{8}$$

$$x_3 \equiv (\lambda(x_1 - x_3) - y_1)(mod\ p) \tag{9}$$

http://www.doi.org/10.62341/rahl1379

iii. Scalar Multiplication.

Suppose K is an integer and $P=(x_1,y_1)$ is a point lies on E . The scalar multiplication can be defined by

$$KP=\underbrace{P+P+\cdots+p}_{K\ times} \quad (10)$$

In other words, adding a point P to itself K times.
A scalar multiplication KP can be computed using the point doubling and point addition laws.

iv. Inverse Operation

Let $P=(x,y)$, then the negative of the point P is

$$Q=-P=(x,-y) \text{ where } P+Q=O.$$

Definition 2.3 The order of an elliptic curve is defined as the number of points of the curve and denoted by $\neq E$.
Definition 2.4 Let P be an element of the elliptic curve group $E(\mathrm{F}_p)$, then P is a generator point if ord $(P)=\#E$.

3. Proposed Hybrid Encryption Scheme

The proposed hybrid encryption scheme combines the block-based algorithm of SOA with the strong asymmetric security mechanisms inherent in elliptic curve cryptography (ECC). Leveraging the algebraic properties of elliptic curves across finite fields, the scheme maintaining computational efficiency suitable for resource constrained environments. The plaintext is divided into fixed size blocks that undergo arithmetic transformations influenced by a dynamically derived key matrix, which is in turn calculated via ECC based key generation combined with a cryptographic coupling or key derivation function. The following algorithm demonstrates the key generation encryption and decryption procedures focusing on the mathematical operations and structural composition that support the system’s security and performance.

Key Generation

- **User A [The sender]**

1. Choose the private key $n_A \in [1, P-1]$.
2. Compute the public key $P_A=n_A.G$.

http://www.doi.org/10.62341/rahl1379

3. Compute the initial key $K_1 = n_A . P_B = (x, y)$.
4. Compute key

$$\pi(x, y) = \frac{(x+y)^2 + 3x + y}{2} = z$$

- **User B [The receiver]**

1.Choose the private key $n_B \in [1, p-1]$.
2. the public key $P_B = n_B . G$.
3.Compute the initial key $K_1 = n_B . P_A = (x, y)$.
4.Compute key

$$\pi(x, y) = \frac{(x+y)^2+3x+y}{2} = z.$$

- **Encryption (User A)**

1. Replace each character in M by its decimal ASCII value.
2. Divided message matrix M into blocks $M_i = \begin{pmatrix} p_1^i \\ p_2^i \end{pmatrix}, i = 1, 2, \dots, m$.
3. Compute $G_j = \begin{pmatrix} g_1^i \\ g_2^i \end{pmatrix} = \begin{pmatrix} p_1^i \\ 2p_1^i + p_2^i \end{pmatrix}, i = 1, 2, \dots, m$.
4. Compute encryption keys E_i

$$E_i = -ZA \pm B = \begin{cases} -ZA + B & i\ odd \\ -ZA - B & i\ even \end{cases}$$

where

$$A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}, \quad E_i = \begin{pmatrix} e_1^i \\ e_2^i \end{pmatrix}, \quad i = 1, 2, \dots, m.$$

5. Encrypt the plaintext, such that

$$C_i = G_i E_i.$$

where C is ciphertext.

6. The numerical ciphertext is stored in a matrix C for transmission.
7.

- **Decryption (User B)**

1. Divided the cipher message matrix C into blocks

$$\begin{pmatrix} c_1^i \\ c_2^i \end{pmatrix}, i = 1, 2, \dots, m.$$

2. Compute the decryption keys

$$D_i = -ZS \pm I = \begin{cases} -ZS + I & i\ odd \\ -ZS - I & i\ even \end{cases}$$

where

$$S = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

3. Encrypt the ciphertext, such that

$$M_i = DC_i,$$

4. Convert the numerical plaintext into its corresponding letter plaintext using ASCII codes.

4. Experimental Results and Analysis

Suppose that user A wants to send a message M to user B and they agreed to use the elliptic curve function

$$\text{E}: y^2 \equiv x^3 + x + 3(mod\ 31),$$

Where $A = 1, B = 1, P = 31$ which satisfies the condition

$$4A^3 + 27B^2 = 4(1)^3 + 27(3)^2 = 4 + 243 = 247\ mod\ 31 = 30 \neq 0,$$

Then the points of the elliptic curve $E_{31}(1,3)$ are shown in Table 1.

TABLE 1. Point on the elliptic curve $E: y^2 \equiv x^3 + x + 3(mod\ 31)$.

(1,6)	(6,15)	(15,13)	(21,4)	(26,11)
(1,25)	(6,16)	(15,18)	(21,27)	(26,20)
(3,8)	(9,11)	(17,2)	(22,3)	(27,11)
(3,23)	(9,20)	(17,29)	(22,28)	(27,20)
(4,3)	(12,10)	(18,5)	(23,14)	(28,2)
(4,28)	(12,21)	(18,26)	(23,17)	(28,29)
(5,3)	(14,8)	(20,5)	(24,5)	(30,1)
(5,28)	(14,23)	(20,26)	(24,26)	(30,36)

Given that the order of the elliptic curve $E_{31}(1,3)$ is 41, which is a prime number any point from Table 1 can be selected as the base point or generator point G. Accordingly, by choosing $G = (1,6)$ the domain parameters for E are defined as

$$\{A, B, p, G\} = \{1,3,31,(1,6)\}$$

For example, let:

$$M = "COVID - 19 "$$

This message will be converted into its ASCLL values, then mapped to the finite field F_p, and finally represented as point on the elliptic curve.
Convert each character into ASCII code:

$$C \to 41, O \to 11, V \to 83, I \to 13, D \to 31, -\to 227, 1 \to 127, 9 \to 167$$

So the ASCII sequence is:

$$P = "41,11,83,13,31,227,127,167"$$

After encoding the plaintext message into numerical values within the finite field, the next step is to generate the elliptic curve keys that will be used in the encryption process.

Step1. Key Generation

User A:

1. Choose the private key $n_{A=}13 \in [1,30]$.
2. Compute the public key $P_A = n_A G$.

$$P_A = 13(1,6) = (3,23)$$

3. Compute initial key $K_i = n_A . P_B$

$$K = 13\ (24,5)\ =\ (20,5)$$

4. Compute key

$$Z = P(20,5) = \frac{(20+5)^2 + 3(20) + 5}{2} = 345$$

User B:

1. Choose the private key $n_{B=}17 \in [1,30]$.
2. Compute the public key $P_B = n_B G$

$$P_B = 17(1,6) = (24,5)$$

3. Compute initial key $K_i = n_B . P_A$

$$K = 17\,(3{,}23) \; = \; (20{,}5)$$

4. Compute key

$$Z = P(20{,}5) = \frac{(20+5)^2 + 3(20) + 5}{2} = 345$$

Step2. Encryption key

$$E_i = -ZA \pm B = \begin{cases} -ZA + B & i\ odd \\ -ZA - B & i\ even \end{cases}$$

$$E_i = -345\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \pm \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$

$$i\ odd,\ E = \begin{pmatrix} -345 & 345 \\ 345 & -345 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -344 & 345 \\ 345 & -344 \end{pmatrix}$$

$$i\ ever,\ E = \begin{pmatrix} -345 & 345 \\ 345 & -345 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} -346 & 345 \\ 345 & -346 \end{pmatrix}$$

Step3. Decryption key

$$D = -ZS \pm I = \begin{cases} -ZS + I & i\ odd \\ -ZS - I & i\ even \end{cases}$$

$$D = -345\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$i\ odd, \qquad D = \begin{pmatrix} -345 & -345 \\ 345 & 345 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -344 & -345 \\ 345 & 346 \end{pmatrix}$$

$$i\ ever, \qquad D = \begin{pmatrix} -345 & -345 \\ 345 & 345 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -346 & -345 \\ 345 & 344 \end{pmatrix}$$

Step4. Encryption

Divide message matrix P into blocks.

To prepare the plaintext for encryption, the message matrix T is divided into smaller blocks of size 2 × 1:

$$P_i = \begin{pmatrix} p_1^i \\ p_2^i \end{pmatrix}$$

Such that

$$P = \text{"41,11,83,13,31,227,127,167"}$$

Then

$$p_1 = \begin{pmatrix} 41 \\ 11 \end{pmatrix}, p_2 = \begin{pmatrix} 83 \\ 13 \end{pmatrix}, p_3 = \begin{pmatrix} 31 \\ 227 \end{pmatrix}, \; p_4 = \begin{pmatrix} 127 \\ 167 \end{pmatrix}$$

Compute

$$G_i = \begin{pmatrix} g_1^i \\ g_2^i \end{pmatrix} = \begin{pmatrix} p_1^i \\ 2p_1^i + p_2^i \end{pmatrix}, i = 1, \dots, 4$$

$$G_1 = \begin{pmatrix} 41 \\ 93 \end{pmatrix}, G_2 = \begin{pmatrix} 83 \\ 179 \end{pmatrix}, G_3 = \begin{pmatrix} 31 \\ 289 \end{pmatrix}, \; G_4 = \begin{pmatrix} 127 \\ 421 \end{pmatrix}$$

Now, we compute ciphertext

$$C_i = E_i G_i$$

We get

$$C_1 = \begin{pmatrix} -344 & 345 \\ 343 & -344 \end{pmatrix}\begin{pmatrix} 41 \\ 93 \end{pmatrix} = \begin{pmatrix} 17981 \\ -17929 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} -346 & 345 \\ 347 & -346 \end{pmatrix}\begin{pmatrix} 83 \\ 179 \end{pmatrix} = \begin{pmatrix} 33037 \\ -33133 \end{pmatrix}$$

$$C_3 = \begin{pmatrix} -344 & 345 \\ 343 & -344 \end{pmatrix}\begin{pmatrix} 31 \\ 289 \end{pmatrix} = \begin{pmatrix} 89041 \\ -88783 \end{pmatrix}$$

$$C_4 = \begin{pmatrix} -346 & 345 \\ 347 & -346 \end{pmatrix}\begin{pmatrix} 127 \\ 421 \end{pmatrix} = \begin{pmatrix} 101303 \\ -101597 \end{pmatrix}$$

Constructing the ciphertext matrix

$$C = \begin{pmatrix} 17981 & 33037 & 89041 & 101303 \\ -17929 & -33133 & -88783 & -101597 \end{pmatrix}$$

Step5. Decryption

Divide the cipher message matrix C into blocks

$$C_{1=}\begin{pmatrix} 17981 \\ -17929 \end{pmatrix}, C_2 = \begin{pmatrix} 33037 \\ -33133 \end{pmatrix}, C_3 = \begin{pmatrix} 89041 \\ -88783 \end{pmatrix}, C_4 = \begin{pmatrix} 101303 \\ -101597 \end{pmatrix}$$

Using the decryption keys D and applying the equation

$$p_i = D_i C_i$$

We obtain

$$p_1 = \begin{pmatrix} -344 & 345 \\ 345 & 346 \end{pmatrix}\begin{pmatrix} 17981 \\ -17929 \end{pmatrix} = \begin{pmatrix} 41 \\ 11 \end{pmatrix}$$

$$p_2 = \begin{pmatrix} -346 & -345 \\ 345 & 344 \end{pmatrix}\begin{pmatrix} 33037 \\ -33133 \end{pmatrix} = \begin{pmatrix} 83 \\ 13 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} -344 & 345 \\ 345 & 346 \end{pmatrix}\begin{pmatrix} 89041 \\ -88783 \end{pmatrix} = \begin{pmatrix} 31 \\ 227 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} -346 & -345 \\ 345 & 344 \end{pmatrix}\begin{pmatrix} 101303 \\ -101597 \end{pmatrix} = \begin{pmatrix} 127 \\ 167 \end{pmatrix}$$

The above plaintext blocks will now be concatenated in matrix.

$$P = \begin{pmatrix} 41 & 83 & 31 & 127 \\ 11 & 13 & 227 & 167 \end{pmatrix}$$

Finally, the plaintext message M is reconstructed as:

$$M = "COVID - 19\,"$$

5. Conclusion

The study proposed a hybrid encryption method that combines the speed and ease of use of SOA with the security benefits of Elliptic Curve Cryptography (ECC). In this implementation, SOA performs fast block encryption, while ECC generates secure keys, a solution to the problem of frequent key exchange in symmetric systems. This is an innovative solution that is both efficient and highly secure. Furthermore, these features make it ideal for applications in constrained environments, such as mobile devices, Internet of Things systems, and real-time applications that require fast operation and high security. Further research could target a hybrid encryption method that combines SOA and RSA key generation algorithms to make SOA even more secure.

Reference

[1] Al-Shabi, M.A., 2019. A survey on symmetric and asymmetric cryptography algorithms in information security. International Journal of Scientific and Research Publications (IJSRP), 9(3), 576-589.

[2] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q., 2020. Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

[3] Ayushi, M., 2010. A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications, 1(15), 1-4. https://doi.org/10.5120/331-502

[4] Annapoorna Shetty, S. S. and K., 2014. A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm. International Journal of Innovative Research in Computer and Communication Engineering, 2(Special issue 5), 98-105.

[5] Chang, X., Li, W., Yan, A., Tsang, P. W. M., & Poon, T. C., 2022. Asymmetric cryptosystem based on optical scanning cryptography and elliptic curve algorithm. Scientific Reports, 12(1), 7722. https://doi.org/10.1038/s41598-022-11861-x

[6] Irzayzah, S. A., Aljalali, O., Altirban, A., & Arebi, R., 2025. SOA Algorithm for Secure Data Encryption and Decryption: A New Random Key-Based Encryption Method. AlQalam Journal of Medical and Applied Sciences, 1864-1871.

[7] Khan, M. R., Upreti, K., Alam, M. I., Khan, H., Siddiqui, S. T., Haque, M., & Parashar, J., 2023. Analysis of Elliptic Curve Cryptography & RSA. Journal of ICT Standardization, 11(4), 355–378. https://doi.org/10.13052/jicts2245-800X.1142

http://www.doi.org/10.62341/rahl1379

[8] Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M., 2018. Elliptic Curve Lightweight Cryptography: A Survey. IEEE Access, 6, 72514-72550. https://doi.org/10.1109/ACCESS.2018.2881444

[9] Rosenberg, A. L., 2003. Efficient pairing functions—and why you should care. International journal of foundations of computer science, 14(01), 3-17.

[10] Yan, Y., 2022. The Overview of Elliptic Curve Cryptography (ECC). Journal of Physics: Conference Series, 2386(1), 1-8. https://doi.org/10.1088/1742-6596/2386/1/012019

[11] Zhou, X., & Tang, X., 2011. Research and implementation of RSA algorithm for encryption and decryption. Proceedings of 2011 6th International Forum on Strategic Technology, 2, 1118–1121.
IEEE. https://doi.org/10.1109/IFOST.2011.6021216