Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 34, Issue 3, 2023 DOI: http://doi.org/10.23851/mjs.v34i3.1318

Research Article **Open Access**

SMS Security by Elliptic Curve and Chaotic Encryption Algorithms

Ziadoon W. Salman[1*], Hind Ibrahim Mohammed[2], Ayman Mohammed Enad
[1]Ministry of Education, Directorate of Education Rusafa-2, 10001 Baghdad, IRAQ.
[2]Al-Mukdad College of Education, University of Diyala, 32001 Diyala, IRAQ.
[3]Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Egypt.

*Correspondent contact: ziadoon.zw.zw@gmail.com

Article Info

Received
23/02/2023

Revised
02/03/2023

Accepted
27/04/2023

Published
30/09/2023

ABSTRACT

Short message services (SMS) represent one of the components of the global communications network and are one of the important developments in communication technologies and communications technology. SMS messages without a password are stored in the SMS server. For the purpose of review and dispute resolution. The security of SMS content cannot be protected because it is transmitted in plain text and is accessible to network operators and employees. Therefore, the end-to-end key is based on encryption and decryption technology can provide SMS security. The security protocols used for SMS security on contemporary mobile devices were examined in this study. SMS security system encryption time affects how well mobile devices work. This shows that security technologies take longer to generate keys and encrypt keys as the key size increases. Due to the limited processing power of mobile devices, large-scale algorithms such as DES, AES, RC4, and Blowfish are not suitable for SMS encryption. SMS may be encrypted using the elliptic curve technique because it provides great security with a smaller key on devices with limited resources, such as mobile phones. And chaotic theory, encryption is simple, fast and secure data encryption. As a result, a combination of elliptic curve algorithm and chaotic encryption algorithm is proposed to achieve a high level of security. In this paper, several tests have been done to compare the algorithms in terms of throughput, power consumption, SMS size, encoding time, and decoding time. The results indicate that the proposed method is better than the comparison method.

KEYWORDS: Elliptic curve algorithm, Encryption, Decryption, Throughput, Security, Chaos theory.

الخلاصة

تمثل خدمات الرسائل القصيرة أحد مكونات شبكة الاتصالات العالمية وهي أحد التطورات الهامة في تقنيات الاتصالات و تكنولوجيا الاتصالات. يتم تخزين رسائل SMS بدون كلمة مرور في مركز خدمة SMS. لغرض المراجعة وتسوية المنازعات. لا يمكن حماية أمان محتوى الرسائل القصيرة نظرًا لأنه ينتقل بنص عادي ويمكن لمشغلي الشبكات والموظفين الوصول إليه. لذلك ، يعتمد المفتاح من طرف إلى طرف على التشفير ويمكن أن توفر تقنية فك التشفير أمان الرسائل القصيرة. تم فحص بروتوكولات الأمان المستخدمة لأمن الرسائل القصيرة على الأجهزة المحمولة المعاصرة في هذه الدراسة. يؤثر وقت تشفير نظام أمان الرسائل القصيرة على مدى جودة عمل الأجهزة المحمولة. يوضح هذا أن تقنيات الأمان تستغرق وقتًا أطول لإنشاء مفاتيح وتشفير المفاتيح مع زيادة حجم المفتاح. نظرًا لقدرة المعالجة المحدودة للأجهزة المحمولة ، فإن الخوارزميات واسعة النطاق مثل DES و AES و RC4 و Blowfish ليست مناسبة لتشفير الرسائل القصيرة. قد يتم تشفير الرسائل القصيرة باستخدام تقنية المنحنى البيضاوي لأنها توفر أمانًا رائعًا بمفتاح أصغر على الأجهزة ذات الموارد المحدودة ، مثل الهواتف المحمولة. والنظرية الفوضوية ، التشفير بسيط وسريع وآمن لتشفير البيانات. نتيجة لذلك ، تم اقتراح مزيج من خوارزميات المنحنى البيضاوي وخوارزمية التشفير الفوضوي لتحقيق مستوى عالٍ من الأمان. في هذه الورقة ، تم إجراء العديد من الاختبارات لمقارنة الخوارزميات من حيث الإنتاجية واستهلاك الطاقة وحجم الرسائل القصيرة ووقت التشفير و وقت فك التشفير. تشير النتائج إلى أن الطريقة المقترحة أفضل من طريقة المقارنة.

Copyright © 2023 *Al-Mustansiriyah Journal of Science*. This work licensed under a Creative Commons Attribution Noncommercial 4.0 International License.

INTRODUCTION

Over the past few years, mobile communication devices have been integrating multiple wireless network technologies to support features and services. They are a popular tool for collecting and disseminating information and data. he SMS service is one of the significant advancements in communication technology [1]. The Global Communication for Mobile Communications system includes SMS in its architecture. The SMS service is one of the significant advancements in communication technology [1]. The Global Communication for Mobile Communications system includes SMS in its architecture. It was originally intended to inform users of their voicemail message, but has now become a popular communications tool by individuals and businesses [2]. Worldwide, banks utilize SMS to conduct various financial operations. Customers can, for instance, use SMS to check the amount of their bank accounts or to make mobile payments. Additionally, people occasionally share sensitive information or secret information like passwords. Voice, data, and fax calls can all be made and received simultaneously with SMS [3]. As a result, SMS is transmitted in plain text, and the privacy of SMS content cannot be guaranteed not only in the air, but also when such messages are saved on the phone. The message's contents are visible to the network operator and users. The reason is that wireless circuits are easier to accept than their wired counterparts [4]. Decoding key is required to easily retrieve the contents of an encrypted signal. A more sophisticated encryption algorithm is harder to eavesdrop on communications without access to the key, which means it's harder to crack a strong password for unauthorized users. Since the fast expansion of wireless and mobile networks, many new applications have been designed and developed for the needs of users. Using wireless networks, information can be transmitted in a more convenient fashion. Wireless networks include many popular techniques [5][6]. In today's environment, data security is critical. Particularly when data is sent across an unsecured communications network. Asymmetric key encryption systems employ a single key for both data encryption and decryption. They are simple in design, but key transfer to the front and multiple key management is a big challenge. It is also difficult to handle keyboards effectively and securely to manage such a large base [7-9].

RELATED WORKS

Many researchers completed early done in the field of SMS security, we will review the most significant studies in this area below:

Muhammad Noman Riaz and, Adeel Ikram (2018) [10] created a secure SMS Android application. To safeguard the data and ensure the safe transmission of private data over the GSM network, cryptographic modification of the data is conducted using the AES 128-bit method. The AES a method is thought to be impenetrable to brute force attacks even by supercomputers. The AES algorithm approach employs perplexing and irregular encryption, rendering data impenetrable to attackers or hackers. This Android software will allow the user to encrypt and decode SMS (Short Message Service) messages with a single click. Following that, an explanation is provided.

Luis Vargas *et al.* (2018) [11] examined more than 900,000 text messages sent to open internet SMS gateways over a period of 28 months, we present a thorough longitudinal research to address these problems. With the use of this information, we can determine where spam is most prevalent and how SMS may be used to spread dangerous material. We can also determine how often benign and malicious SMS ecosystem behaviors vary over time. The most important conclusions from this study are that many services send sensitive security-related messages over unencrypted channels, employ low entropy solutions for one-use codes, and behave in ways that suggest public gateways are primarily used to get around rules requiring verified phone numbers for account creation. This latter discovery reveals that such evasion exists and has important implications for preventing phone-verified account fraud.

Bosung Kim,and Jooseok Song (2019) [12] resolved the security flaws of earlier research, we provide an energy-efficient and secure mobile node authentication system (ESMR) for MWSNs. This approach meets the security

criteria of MWSNs and is suitable for mobile wireless sensor networks. By allowing a foreign cluster head to authenticate mobile nodes, ESMR eliminates unconditional forwarding and offers high-compromise resilience by limiting the usage of cryptographic keys for various functions. The results of a security study demonstrate that ESMR satisfies security standards and can thwart pertinent security assaults. In multi-hop communication environments, where there are two or more hops between the mobile node and cluster head, performance evaluations demonstrate the suitability of ESMR. In particular, ESMR introduces little performance overhead because it only necessitates less than 6% more overall energy usage and 3% more authentication delay than in earlier research. Considering both performance and security aspects, ESMR also can be applied to single-hop communication environment.

Srinivas Jangirala *et al*. (2020) [13] designed LBRAPS, a novel effective and lightweight authentication system for supply chains in a 5G mobile edge computing context. Only bitwise rotation, one-way cryptographic hash, and bitwise exclusive-or (XOR) operations are used in LBRAPS. LBRAPS has proven to be protected from a number of assaults. LBRAPS security is further guaranteed by the simulation-based formal security verification carried out utilizing the widely used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Finally, it is demonstrated that, when compared to current protocols, LBRAPS offers a superior trade-off between its security and functionality features, communication and computing costs.

Rakesh Shrestha *et al*. (2020) [14] suggested a specific kind of block chain to address important message propagation problems in the VANET. We develop a brand-new kind of block chain that is appropriate for the VANET called a local block chain for real-world event message transmission among vehicles inside the borders of a nation. We describe a distributed ledger that is suitable for safe message distribution that records the node trustworthiness and message trustworthiness in a public block chain.

Sylfania *et al*. (2020) [15] introduced the RSA and Blowfish algorithms into the Android application-based sending and receiving of emails. To identify whether method has exceptional speed, both algorithms will be analyzed and compared in terms of encryption and decryption speed. The Blowfish method was chosen because it was the fastest and produced the best results when compared to other symmetric algorithms. The RSA algorithm is chosen because it executes more quickly than other asymmetric algorithms. Calculating the encryption and decryption times for two methods with the same key length and message character set is a test method. Measure the passage of time 10 times, then average the results to obtain a reliable result. According to the study's findings, the Blowfish algorithm is quicker than the RSA method. the examination. The test results showed that Blowfish was 178,958% quicker than RSA in encrypting data. In contrast, Blowfish is 63.131% faster than RSA. The same outcome is obtained for the decryption procedure, with Blowfish being quicker than 420.44188% compared to RSA. RSA is 80.3399% slower than Blowfish, on the other hand.

Saman Shojae Chaeikar *et al*. (2021) [16] developed a technique for protecting short message communications is presented that generates two distinct and dynamic encryption and decryption keys using four prominent cryptographic key generation parameters. The evaluation results demonstrate that the suggested method employs secure encryption and decryption keys, is resistant to a variety of cryptographic and network attacks, significantly lowers the cost of establishing secure sessions, and provides a high level of usability and security that is well received by the users.

The Proposed ECCT Algorithm

The proposed algorithm consists of two parts: pre-processing by the chaos system and ECC encryption. The clear text will be processed by chaotic sequences after exiting the ECC encryption system. The proposed system uses elliptic curve encryption and a chaos system to encrypt the message and send it on a shared

Copyright © 2023 *Al-Mustansiriyah Journal of Science*. This work licensed under a Creative Commons Attribution Noncommercial4.0 International License.

channel. The sender composes a message and provides the recipient's phone number; when the message is sent, the algorithm is activated on both devices. The keys are generated and distributed to the devices, and encryption is performed on end-to-end transmitters. The key syntax between the transmitter and the receiver is fully described in the next section. After encoding using ECC, decoding encryption methods in ECC are designed to encode and decode a curve point, not the whole message. In encryption, each character in the message is transformed to bytes, which are then turned to points of the type (y, x), which must then be coded by mapping each of them to each point on the elliptic curve and Because SMS can only contain string values, all encoded points must be transformed to bytes and subsequently to strings.

The encrypted text is entered into the turmoil system and generates a few encrypted texts as a clear text for the ECCT algorithm. In order to make it harder for decryption to the hackers, the message is sent to the receiver and he uses it using his chaos system Decrypts the text used in chip output in decoded text as encoded text for the ECCT algorithm. When the message reaches the receiver, during the decryption process, the string must be converted to bytes; these bytes must be Spots are decrypted again using ECC and then points to bytes and eventually cache turn up the message and only then decrypted plaintext can be viewed by the recipient. The general scheme of the proposed method is shown in Figure 1 and Algorithms 1 and 2 show the stages of the proposed method.

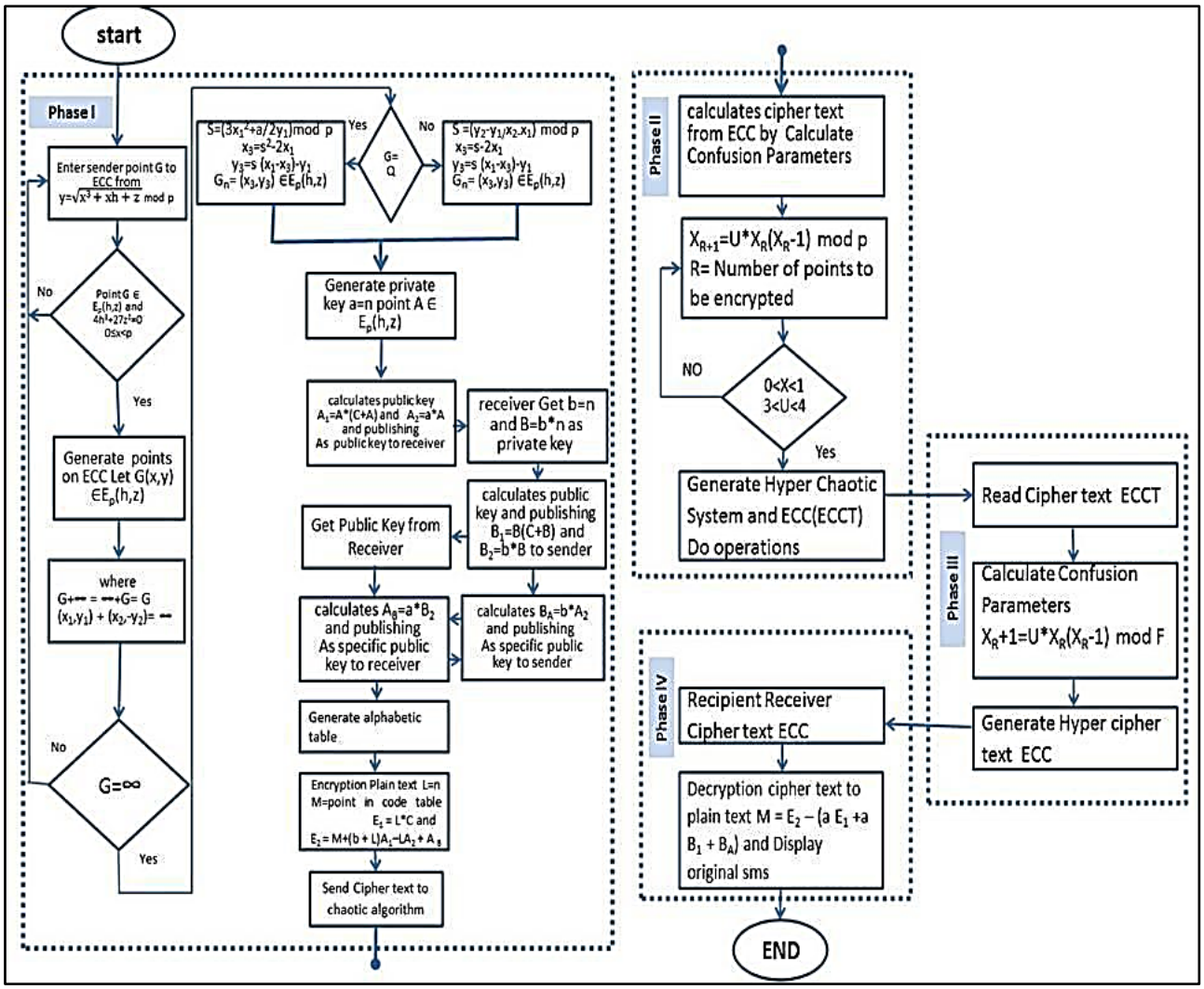

Figure 1: The proposed ECCT algorithm

Algorithm1: Elliptic Curve and Chaotic Encryption (ECCE) Algorithms (sender)

Input: Message (Plain text)
Output: Cipher text and general public

Step1: Generating points G ∈ E_p (h, z) on Elliptic curve algorithm by the equation $y=\sqrt{x3 + xh + z}$ mod p. h, z: integer number p: primary number.
Step2: Encryption SMS uses ECC algorithm. by condition Point G ∈ E_p (h, z), $4h^3+27z^2\neq 0$ and $0\leq x<p$.
Step3: In case G + ∞ = ∞+G =G for all E_p (h, z), where ∞ is the point at infinity. and G (x, y) ∈ E_p (h,z) then(x,y) + (x,-y) = ∞. Where (x, -y) is the negative of G, denoted by –G.
Step4: in case G=∞ GOTO step 2 else GOTO step 5.
Step5: computes a= random number and the point A as her private keys.
Step6: if G (x_1, y_1) =Q (x_2, y_2) ∈ E_p (h, z) then GOTO step 7 else GOTO step 8.
Step7: in case G (x_1, y_1) =Q (x_2, y_2) ∈ E_p (h, z) G≠-G Then G+Q= (x_3, y_3). $S=(3x_1^2+a/2y_1)$ mod p $x_3=s^2\ 2x_1 \text{mod} p$ $y_3=s(x_1-x_3)-y_1$ mod p.
Step8: in case G (x_1, y_1) =Q (x_2, y_2) ∈ E_p (h, z) G≠-G Then G+Q= (x_3, y_3). $S=(3x_1^2+a/2y_1)$ mod p $x_3=s-2x_1$ mod p $y_3=s(x_1-x_3)-y_1$ mod p.
Step9: private key 1 = a, a random number less than the order of the generator. Private key 2 = a point A on the elliptic curve E_p (h, z).
Step10: Let points C, A1, A2 on the elliptic curve E_p (h, z) general public key$_1$=a, Point $A_1=A*(C+A)$ and general public key 2 = a point $A_2=a*A$. And publishing as public key to the receiver.
Step11: private key 1 = b, a random number less than the order of the generator. Private key 2 = at point B on the elliptic curve E_p (h, z).
Step12: general public key 1 = a point $B_1=B*(C+B)$ and general public key 2 = a point $B_2=b*B$ on the Elliptic curve E_p (h, z). And publishing as public key to send.
Step13: End

Algorithm2: Elliptic Curve and Chaotic Encryption (ECCE) Algorithms (server)

Input: Cipher text and general public
Output: plain text

Step1: Get pair Public Key (B1, B2) from the Receiver.
Step2: sender sends the encrypted secret key $AB=a*B_2$ to receiver in a public channel.
Step3: server sends the encrypted secret key $BA=b*A_2$ to sender in a public channel.
Step4: Generate appropriate alphabetic table Read the table in row-major form and find the character stored in that position an appropriate data structure to store the text to be encrypted.
Step5: Using the agreed-upon coding table, the sender turns all of the message's text characters into points on elliptic curves. Encrypt the message M then all the characters of the dispatch he selects a random number L for encrypting the character. Then each message point is encrypted to a pair of cipher points $E_1 = L*C$, $E_2 = M+(b + L) A_1 – L A_2 + A_B$.
Step6: Send Cipher text ECC to phase2.
Step7: a chaotic algorithm modification Place the original x and y values in a two-dimensional table so that each array element is integer.
Step8: Apply the selected transformation on the table for a number of steps specified by the equation $X_{R+1}=U*X_R (X_R-1)$ mod p R=Number of points to be encrypted.
Step9: IF $0<X<1$ and $3<U<4$ go to step 10 else come back step 7.
Step10: converts all the points of the ECC into points Consists of a different pair its name (ECCT).
Step11: Apply decryption process Read Cipher text ECCT.
Step12: Anyone with the key can decrypt the data just as easily. Simply reverse the steps and apply inverse transformations to the same number of steps.
Step13: Return to cipher text if ECC original.
Step14: Recipient Receiver Cipher text ECC from chaotic algorithm.
Step15: To convert Decrypted cipher text to plain text equation is used $M= E_2 – (an E_1 + a B_1 + B_A)$ and display original SMS.
Step16: End.

Evaluation of Parameters

We chose the following parameters for evaluating the combination ECCT against the combination of RSA + chaotic encryption algorithms for both encryption and decryption schemes:

1. Encryption time: (Encryption time = Simple text encryption time / Time to receive encrypted text (Computation time / response time) The encryption time is the time when the cryptographic algorithm considers a simple text to generate a cipher text.
2. Decryption time: (decoding time = decoding time of encryption / time text to get plain text (Computation time / response time) decoding time is when an encryption algorithm takes into account the reproduction of plain text from an encrypted text.
3. Throughput:

Copyright © 2023 *Al-Mustansiriyah Journal of Science*. This work licensed under a Creative Commons Attribution Noncommercial4.0 International License.

- (Power Capture Cipher = Full Plain Text in Encrypted Bits / Encryption Time) The operating power is equal to the total of plain text in encrypted bits divided by the encryption time Higher operating efficiency will increase efficiency.
- (Decoding power = total encoded text in decoded bits / decoding time)

The operational power is equal to the total encoded text in decoded bits divided by decoding time Higher operating efficiency will increase efficiency.

RESULTS AND DISCUSSION

In this research, three significant measures are described for estimating the efficiency of the proposed algorithm (ECCT). The criteria are: encryption time, decryption time and operational capability. The test is then performed and the performance results are measured using the HUAWEI RIO-L01 mobile phone for comparison with ECCT and RSA algorithms (RSA+ chaotic).

Encryption time

Figure 2 shows the comparison of encryption time. The X axis represents the number of SMS characters and the SMS number for each SMS = 160 characters. The secondary Y axis is the encryption time of all algorithms. ECCT shows better performance over a (chaotic+ RSA) during encryption.

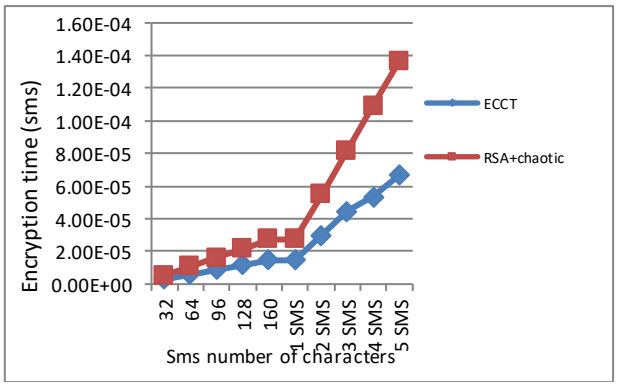

Figure 2: Comparing encoding time in ECCT and chaotic+ RSA based on the number of SMS characters.

Decryption time

Figure 3 shows the comparison of decoding time. The X axis represents the number of SMS characters and the number of SMS for each SMS = 160 characters. The secondary Y axis is the decoding time of all algorithms. ECCT shows better performance over chaotic+ RSA in terms of decoding time.

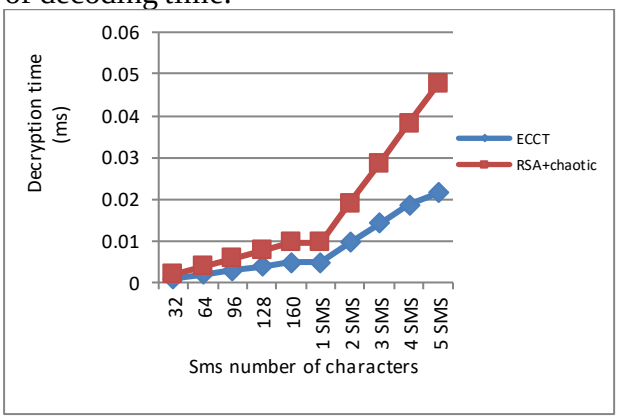

Figure 3. Comparing decoding time in ECCT + RSA based on the number of SMS characters.

Throughput

Power Encryption Time

The encryption time is considered when the encryption algorithm generates a plain text from a plain text. The encryption time is used to calculate the power of an encryption, as a whole simple text in encrypted bits divided by encryption time. A comparative analysis of the results of the selected cryptographic scheme is performed.

Figure 4 shows the comparison between ECCT, and (chaotic+ RSA) ECCT for the encryption process. Comparison of the operating power indicates that the X axis represents the number of SMS characters and the number of SMS per SMS = 160 characters. The secondary Y axis is the encryption time of all algorithms. It is concluded that the ECCT shows better performance than chaotic+ RSA in the encryption process.

Figure 4: Comparison of the time zone between the ECCT and chaotic+ RSA

Throughput decryption time

The decoding time is considered when a decryption algorithm encodes a text to produce a plain text. The decoding time is used to calculate the power of a decoding scheme, so that the entire encoded text is calculated in decoded bits divided by decoding time. A comparative analysis is performed on the results of the selected decoding scheme. Figure 5 shows the comparison of the power between ECCT, and (chaotic+ RSA) for the decoding process. Compares the power of the show. Axis X represents the number of SMS characters and the number of SMS for each SMS = 160 characters. The secondary Y axis is the decoding time of all algorithms. We conclude that the ECCT in the process of decoding power is better than (chaotic+ RSA).

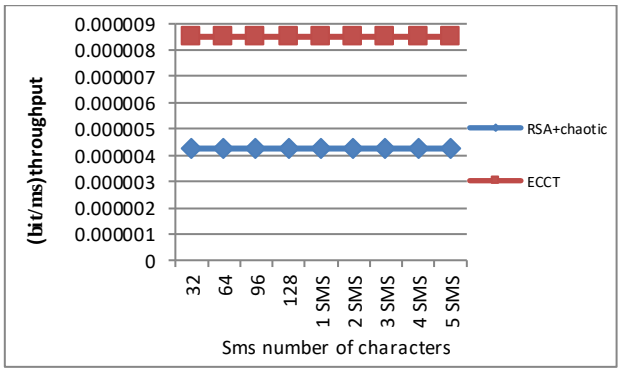

Figure 5. Comparison of decoding power between ECC and chaotic+ RSA based on the number of SMS characters

CONCLUSIONS

The Elliptic Curve encryption algorithm with SMS integration is valuable due to its high security level despite utilizing smaller key sizes suitable for devices with limited resources, such as mobile phones. This algorithm is grounded in chaos theory and is based on various mapping techniques, including logistic mapping, Baker mapping, circle mapping, Gauss mapping, Henon mapping, and more. In our thesis, we specifically employed logistic mapping. This algorithm is characterized by its simplicity, speed, and data security features, making it an excellent choice for data encryption. Consequently, combining these two Elliptic Curve and chaos encryption algorithms enhances overall security. In summary, the results we have obtained are as follows:

- ECCT excels in both encryption and decryption times. When compared to the encoding and decoding times of chaotic algorithms combined with RSA, the ECCT algorithm proves to be faster.
- Operational power is a critical parameter that illustrates the performance of each algorithm.
- ECCT outperforms (chaotic algorithms + RSA) in terms of throughput during the encryption and decryption processes.

Disclosure and Conflicts of Interest: The authors advertise that they have no conflicts of interest.

REFERENCES

[1] Shoewu, O., and Segun O. Olatinwo. "Securing Text Messages using Elliptic Curve Cryptography Orthogonal Frequency Division Multiplexing." Pac. J. Sci. Technol.Vol.14,nu.2,November 2013.

[2] Sridhar C. Iyer, R.R.Sedamkar,ShiwaniGupta"Multimedia Encryption using Hybrid Cryptographic Approach" International Journal of Computer Applications, 2014, pp. 0975 – 8887.

[3] Fang Yuan, Guang-Yi Wang, and Bo-zhen Cai. "Android SMS encryption system based on chaos." 2015 IEEE 16th International Conference on Communication Technology (ICCT). IEEE, 2015, pp. 856 - 862.

[4] BHIMRAO PATIL."SMS SECURITY USING RC4 & AES." Indian J. Sci. Res 11.1,2015, pp. 034-038.

[5] RashmiRamesh Chavan, and Manoj Sabnees."Secured mobile messaging." Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on. IEEE, 2012, pp. 1036-1043

[6] Muhammad Murad Khan, Majid Bakhtiari, Saeid Bakhtiari. "An HTTPS approach to resist man in the middle attack in secure SMS using ECC and RSA." 2013 13th International Conference on Intelligent Systems Design and Applications. IEEE, 2013, pp. 115-120.

[7] Sri Rangarajan, N.Sai Ram, N. Vamshi Krishna. "Securing SMS using Cryptography." International Journal of Computer Science and Information Technologies (IJCSIT) 4.2 ,Vol. 4 (2), 2013, pp. 285-288.

Copyright © 2023 *Al-Mustansiriyah Journal of Science*. This work licensed under a Creative Commons Attribution Noncommercial4.0 International License.

[8] M. Shanmugasundaram, and R. Shanmugasundaram. "Elliptic Curve Cryptography (ECC) for Security in Mobile Communication." European Journal of Advances in Engineering and Technology 1.2, 2014, pp.93-101.

[9] Nimmya Unnikrishnan, and Divya K. V." End to End Secure SMS Communication: A Literature Survey.", Vol. 4, 2015, pp, 2347 – 8616.

[10] Riaz, Muhammad Noman, and Adeel Ikram. "Development of a secure SMS application using advanced encryption standard (AES) on android platform." *Int. J. Math. Sci. Comput. (IJMSC)* 4.2 (2018): 34-48.

[11] Reaves, Bradley, et al. "Characterizing the security of the SMS ecosystem with public gateways." *ACM Transactions on Privacy and Security (TOPS)* 22.1 (2018): 1-31.

[12] Kim, BoSung, and JooSeok Song. "Energy-efficient and secure mobile node reauthentication scheme for mobile wireless sensor networks." *EURASIP Journal on Wireless Communications and Networking* 2019 (2019): 1-16.

[13] Srinivas, Jangirala, and Ashok Kumar Das. "Lightweight Security Protocols for Blockchain Technology." *Cyber Defense Mechanisms*. CRC Press, 2020. 131-156.

[14] Shrestha, Rakesh, et al. "Evolution of V2X communication and integration of blockchain for security enhancements." *Electronics* 9.9 (2020): 1338.

[15] SYLFANIA, Dwi Yuny, Fransiskus Panca JUNIAWAN, and Harrizki Arie PRADANA. "Blowfish–RSA Comparison Analysis of the Encrypt Decrypt Process in Android-Based Email Application." *Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)*. Atlantis Press, 2020.

[16] Chaeikar, Saman Shojae, Saeed Yazdanpanah, and Nakisa Shoja Chaeikar. "Secure SMS transmission based on social network messages." *International Journal of Internet Technology and Secured Transactions* 11.2 (2021): 176-192.

How to Cite

Z. W. Salman, H. I. . Mohammed, and A. M. . . Enad, “SMS Security by Elliptic Curve and Chaotic Encryption Algorithms”, Al-Mustansiriyah Journal of Science, vol. 34, no. 3, pp. 56–63, Sep. 2023.