Analysis of Elliptic Curve Cryptography & RSA

Mohammad Rafeek Khan[1], Kamal Upreti[2,*],
Mohammad Imran Alam[1], Haneef Khan[1],
Shams Tabrez Siddiqui[3], Mustafizul Haque[4]
and Jyoti Parashar[5]

[1]*Department of Computer & Network Engineering, CS & IT College, Jazan University, 45142, KSA*
[2]*Department of Computer Science, CHRIST (Deemed to be University), Delhi NCR, Ghaziabad, India*
[3]*Department of Computer Science, CS & IT College, Jazan University, 45142, KSA*
[4]*Dr. D.Y. Patil Vidyapeeth's Centre for Online Learning, Dr. D.Y. Patil Vidyapeeth, Pune (Deemed to be University), India*
[5]*Dept. of Computer Science & Engineering, Dr. Akhilesh Das Gupta Institute of Technology & Management, GGSIPU, New Delhi, India*
E-mail: mokhan@jazanu.edu.sa; kamalupreti1989@gmail.com; mimran@jazanu.edu.sa; haneeskhan@jazanu.edu.sa; stabrez@jazanu.edu.sa; mustafizulhaque84@gmail.com; jyoti.parashar123@gmail.com
**Corresponding Author*

Received 15 April 2023; Accepted 27 August 2023;
Publication 18 November 2023

Abstract

In today's digital world, the Internet is an essential component of communication networks. It provides a platform for quickly exchanging information among communicating parties. There is a risk of unauthorized persons gaining access to our sensitive information while it is being transmitted. Cryptography is one of the most effective and efficient strategies for protecting our

Journal of ICT Standardization, Vol. 11_4, 355–378.
doi: 10.13052/jicts2245-800X.1142

data and it are utilized all around the world. The efficiency of a cryptography algorithm is determined by a number of parameters, one of which is the length of the key. For cryptography, key (public/private) is an essential part. To provide robust security, RSA takes larger key size. If we use larger key size, the processing performance will be slowed. As a result, processing speed will decrease and memory consumption will increase. Due to this, cryptographic algorithms with smaller key size and higher security are becoming more popular. Out of the cryptographic algorithms, Elliptic Curve Cryptography (ECC) provides equivalent level of safety which RSA provides, but it takes smaller key size. On the basis of key size, our work focused on, studied, and compared the efficacy in terms of security among the well-known public key cryptography algorithms, namely ECC (Elliptic Curve Cryptography) and RSA (Rivets Shamir Adelman).

Keywords: Cryptograph, RSA, elliptic curve cryptography, public key cryptography, security.

1 Introduction

The importance of cryptography in data security cannot be ignored. Cryptography is the process of sending sensitive information through insecure networks such as the internet in such a way that it cannot be read by anybody other than the person to whom it is being sent. It essentially hides the data. Cryptography provides a number of security goals, including data privacy and non-alteration. Cryptography is frequently employed today due to its significant security benefits. The various goals of cryptography are listed below: Confidentiality: Information stored in a computer is sent out and can only be viewed by those who have been given permission to do so. Authentication: Any system that receives data must verify the sender's identity to determine if the data is coming from a legitimate source or a fake identity. Integrity: Only the individual to whom we are sending the message has access to the information that is being delivered. Non-repudiation: Information once transmitted, it can't be denied either by sender or recipient. Access Control: The information is only accessible to those who have been given permission. Cryptographic algorithms have been categorized as: Symmetric Encryption (Private Key Cryptography) and Asymmetric Encryption (Public Key Cryptography). Symmetric Encryption Cryptography requires only a single key that is been shared between the sender and the receiver. The encryption is performed on the message in order to encrypt and produce a cipher text

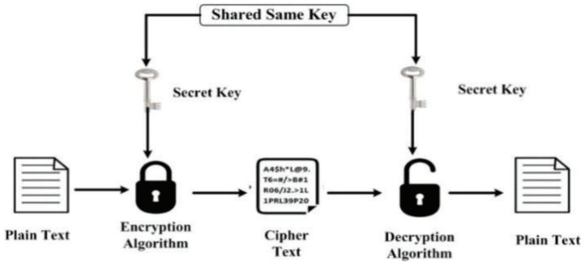

Figure 1 Symmetric cryptography.

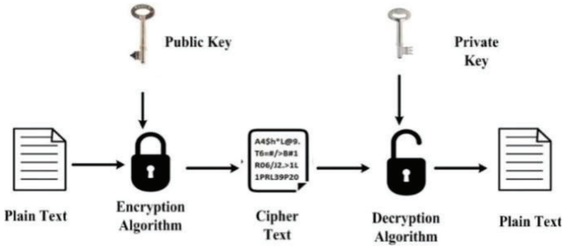

Figure 2 Public key algorithm.

whereas decryption is performed on the message to decrypt and produce a plain text as shown in Figure 1 [3].

In asymmetric key cryptography two keys are needed: private keys and public keys. A public key is used to create the cipher text produced by encryption, while a private key is used to create the plain text obtained by decryption. Everyone has access to the public key, but the private key is only accessible by the user. A public key can be used to decrypt a communication that has been encrypted with a private key. A message encrypted with a public key, on the other hand, with a private key can it be decrypted. This provides additional protection against malicious users during data transfer [1]. In RSA, Daffier-Hellman, and Elliptic curve cryptography are types of public key cryptography algorithms. Figure 2 displays the asymmetric (public key) cryptography model.

All senders and receivers in symmetric cryptography are using the same key and encryption technique. In a situation where either the sender or the receiver's key is compromised or leaked, the entire communication is breached. However, in Public Key Encryption, either of the parties shares keys that are publicly and privately available to everyone. (Just the sender's private key), assuring the message's security [1].

As a result, asymmetric cryptography is used for encryption in the majority of block chain applications, such as Bitcoin, Ethereum, and other crypto currencies. Despite having a similar framework, public-key cryptography, which is utilized in the block chain, is considered to be appropriately and effectively functioning well besides the symmetric encryption technique [2].

RSA Public Key Cryptography: Only two years after the foundational Diffie–Hellman work was published; the first public-key encryption technique was made public in 1978. It's called RSA after its inventors' initials, R. Rivest, A. Shamir, and L. Adleman, and it's still the most significant and frequently used public-key encryption method today, with several variants included in several standards. Following that, we'll talk about this scheme and its security mechanisms. The other key, on the other side, is a private key that will be used to decipher the encipher text. Public encryption differs from symmetric encryption, It uses the same key for both enciphering & deciphering [8, 9]. The primary benefit of using an asym metric encryption key is that it provides strong encryption that makes decryption of the actual text is a challenge and difficult for hackers to predict [15].

2 Literature Review

In this paper, the RSA and ECC algorithms are compared on the basis of the keys structure namely its size, its performance both in generation and verification of the keys with supportive findings suggests that ECC has shown better results than RSA [1].

Author suggests the ECC cryptography method is used to develop a group security mechanism. ECC uses group security in the form of m-gram selection, which is referred to as ECC m-gram selection. In compared to individual item security, processing speed will be faster due to the implementation of group security in terms of common grams [7].

Here authors suggest and concludes that the performance of ECC offers better results and has proven to be beneficial for SSL clients and servers therefore focusing on enhancing the security. Significantly, block ciphers employ the Advanced Encryption Standard (AES), which employs 128,192, and 256-bit keys are available. The most efficient PKC algorithms among all asymmetric encryption techniques are RSA and ECC. They favoured it because of its superior performance compared to other asymmetric algorithms [11]. As a result, we concentrate on RSA vs ECC using key sizes of ECC uses 160 bits and RSA uses 1024 bits. This has proven to be more beneficial for devices that will show better performance with same level of security [12]. The performance of QR Code Authentication with RSA and Elliptic Curve Cryptography is compared in this research. Web applications, mobile applications, one-time passwords, Elliptic curve cryptography, and Asymmetric key algorithms are among the techniques and ideas used in the investigation. The main goal of this research is to present a quick and easy way to authenticate QR codes that is both secure and performs well technically [14, 25].

This paper discusses the ECC encryption technique and shows an example of how it is implemented. ECC is used for encryption, key exchange, IoT & smart cards applications other secure communications. ECC utilizes significantly less memory, and pair of keys generation and signing are significantly faster [16, 24]. Elliptic cryptographic curves' strength is revealed by comparing RSA with ECC in terms of performance. Additionally, this article uses random private keys and varied key bit sizes to implement RSA and ECC [29]. ECC aspires to thoroughly examine a wide range of scientific ideas, cutting-edge technologies, and original approaches. ECC is more secure than RSA and the Diffie-Hellman algorithm and can be used in cloud computing, e-health, and electronic voting [30].

To increase the effectiveness and speed of RSA decryption, Boneh et al.'s [31] survey involving four RSA variants was done. They used a 1024-bit RSA modulus to assess these variations. Their results show that two multi-factor RSA algorithms ($n = p^2q$ and $n = pqr$) and batch RSA are entirely backward-compatible. Additionally, when the encryption-exponent 'e' is big, the adjusted RSA technique provides significantly greater efficiency gains. As a substitute to the Euclidean Algorithm, Chang et al. [32] developed an efficient parallel method for creating RSA keys utilising Derome's technique. Authors asserted that their approach requires little computational energy to operate.

According to Verma et al. [33], they were able to generate both a modulus and a key by employing only a few orders of the matrix. They discovered that a matrix of four order is adequate to provide a confidential RSA key and around 840-bit modulus. Their model utilised the Chinese Remainder Theorem (CRT) in order to speed up deciphering in addition to a short encrypted exponent to hasten up encryption. Ahmad et al.'s [34] variation of RSA encryption uses CRT to compress several plaintexts and hide them within a single ciphertext. They showed how the algorithm might withstand several security breaches and put up fixes for additional security problems. Whenever an individual develops 'n' instance with the identical modulus, Santosh et al. [35] asserted that such instances may disable Multi-prime RSA via lattice basis reduction.

An enhanced threshold authentication technique built on RSA with CRT was proposed by Dong et al. [36]. They reasoned that because every participant generates their secret shadows individually and may confirm the validity of secret shadows generated by others, their technique doesn't call for an encrypted communications route. For the (δ, β)-SIP problem, Takayasu et al. [37] offered an improved lattice architecture. Their findings showed that Multi-Prime RSA becomes greater in sensitivity than anticipated if the discrepancies between the prime factors are minimal.

Techniques for Elliptic Curve Cryptography (ECC) were put into effect by Bhardwaj et al. [38], with an emphasis on, point addition, scalar multiplication and point doubling. Additionally, they evaluated the efficiency of ElGamal both in encryption and decryption across an area of finite size. An investigation on an ECC-based protocol for security for Radio Frequency Identification (RFID) devices was done by Qian et al. [39]. They emphasised a number of benefits of utilising ECC, including offering adequate safety to facilitate communication and label memory information access, lowering the amount of key space needed by preserving just private keys, and leveraging effective bitwise operations to reduce tag calculation. BAN-logic was used to examine the protocol's security measures, formal evidence and computational efficiency. In order to cut down on the amount of elementary operations in ECC, Basu [40] suggested a transformation technique. To further lower the cost of computation, they used concatenation phases and parallel computing, attaining speeds that were almost to the order of N, whereby N is the total number of processors. On the basis of the characteristics of isogenies between super-singular elliptical curves, Srinath et al. [41] suggested an Udeniable Blind Signature Scheme (UBSS). Considering certain presumptions, they demonstrated that their system is still reliable despite being in the face of a quantum attacker.

3 Ellipic Curve Cryptography

ECC was created in 1985 by N. Koblitz and Miller, who employed an elliptical curve to accomplish cryptographic encryptions (ECC) [13]. Similar to the Public key encryption, in ECC, both the parties acquire publicly and privately a pair of keys which is used for enciphering & deciphering [27]. We consider a large prime number p and Fp is considered as the modulus of the integers used in p.

Upon observing the graph, an elliptic E (curve) is formed on Fp. It is formulated by an expression:

$$\mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} + \mathrm{b}, \tag{1}$$

in this expression: a, b are defined as the integers used in modulus Fp. upon the condition,

In such a way that $4\mathrm{a}^3 + 27\mathrm{b}^2 \neq 0$ (mod p)

If (x, y) satisfy the equation, then the pair (x, y) is a point on the curve (1). The curve also includes the infinity point, which is denoted by. The letter E stands for the set of all points on E. (Fp).

Consider the case when E is an elliptic curve with the following defining equation:

$$\mathrm{y}^2 = \mathrm{x}^3 - 5\mathrm{x} + 2, \tag{2}$$

The following graph (Figure 3) for an elliptic curve is plotted using Equation (2).

A private key is a random number, while a public key is a point on the curve. Multiplying the private key by the curve's generator point G yields the public key. The domain parameter of ECC [6] is made up of G is the generator point, a and b are the curve parameters, and there are a few other constants. RSA is being used in the vast majority of public-key cryptography products and standards for encryption and digital signatures. The bit length for secure RSA use has risen over the years, putting a larger processing burden on systems that use this algorithm. The usage of this algorithm has overwhelmed the proper functioning, especially for the e-commerce websites that are prone

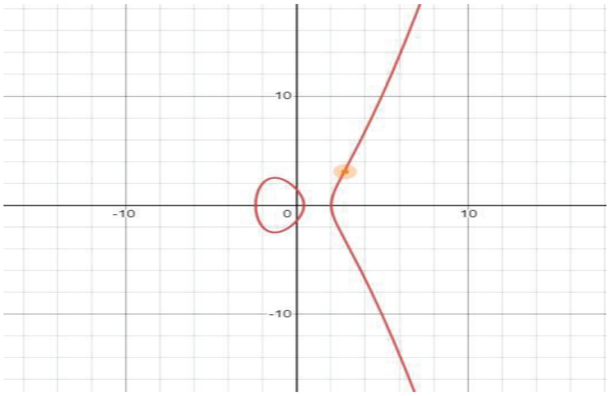

Figure 3 Elliptic curve.

to deal with voluminous and secured transactions [17, 26]. For this reason, a comparative study between RSA and ECC was done, which resulted to be beneficial for ECC, although the level of security was equally the same, but the data size that was considered was of smaller bit size, due to which the processing time was comparatively less than RSA [5, 28].

The disadvantage of lengthy key sizes in conventional cryptographic systems, such as RSA, is addressed by elliptic curve cryptography (ECC), which provides equivalent security with shorter key lengths. ECC methods execute computations on groups related to the elliptic curve rather than the huge numbers utilised in RSA, allowing for smooth integration with public key cryptography. Given that solving the discrete logarithm problem on the elliptic curve group is thought to be more complicated than factoring huge numbers into primes, this method makes it far more difficult to break digital signatures through ECC.

Data is encrypted and decrypted using public and private keys in asymmetric cryptography, sometimes referred to as public key cryptography. These keys are made up of big numerals that are paired off but are not the same (asymmetrically). While the private key is kept secret, the public key can be shared with everyone. Either key may be used for encryption, or the key used for decryption must be the opposite of the key used for encryption. This strategy is demonstrated by asymmetric key cryptosystems like RSA, ELGAMAL, and ECC [42].

In Section 2 literature review of two algorithms i.e. RSA and ECC is discussed. In the next section, we discussed the comparative analysis of RSA and ECC, in Section 4 experiment is conducted for both the algorithms on different parameters and evaluated the performances of both algorithms namely RSA and ECC. In the last Section 5, we discussed the conclusion and future direction of this study [18].

4 ECC and RSA Algorithms

We compared In terms of key creation, encryption, and decryption (ECC vs RSA), and aggregated these three factors in terms of time performance in this work [19]. We used Maple soft and a computer system with the following configuration for this analysis:

System: 64-bit OS (operating system), x64-(based processor), and Windows (10 version) installed Processor: Intel Core i7 CPU with 1.80 GHz 1.99 GHz and that of RAM is 8.00 Giga byte.

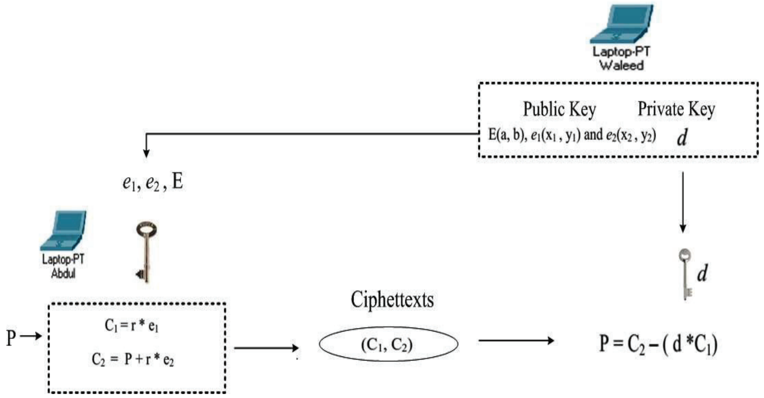

Figure 4 Elliptic curve cryptography (ElGamal).

4.1 Elliptic Curve Cryptography using Megamall

We employed the Megamall approach for encryption and decryption techniques in this paper, which uses an elliptic curve on Galois Field (GF) (2n) as shown in Figures 4 and 5.

Procedure for Generating Public and Private keys ECC.

On the elliptic curve, Waleed chooses E(a, b) above GF (2n).

Waleed chooses a point on the curve to work with.

Waleed chooses the integer d.

Waleed determines that $e_2(x_2, y_2) = d * e_1(x_1, y_1)$ (means adding points d times).

Waleed declares his public keys as E(a, b), $e_1(x_1, y_1)$, and $e_2(x_2, y_2)$, and his private key as.

Procedure for Encryption ECC.

Abdul chooses P as simple text on the elliptic curve.

Abdul calculate pair of ciphertext on the plain text p by using the following formula

$$C_1 = r * e_1$$

$$C_2 = P + r * e_2$$

Abdul send two cipher text (C_1, C_2) to Walled.

4.1.1 Procedure for decryption ECC

Waleed receives (C_1, C_2) as a ciphertext.

Waleed calculates P (Plain text) by using following formula:

$$P = C_2 - (d * C_1)$$

4.2 RSA Cryptographic Algorithm

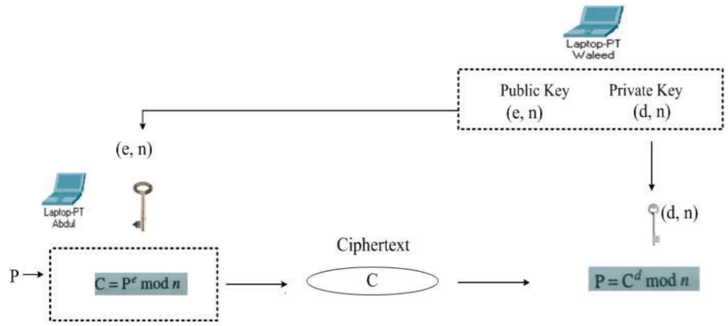

Figure 5 RSA algorithm.

4.2.1 Procedure for generating public and private keys

Waleed selects two big prime numbers p and q ($p \neq q$)

Waleed calculates $n = p*q$;

Now calculates $m = (p - 1)(q - 1)$;

Choose e so that both e and m are prime numbers.

Calculate d, in this way $d*e \text{ Mod } m = 1$

Waleed calculates Public key and private key as follows:

$$\text{Public key} = \{e, n\}$$
$$\text{Private key} = \{d, n\}$$

Waleed declares e to be public-key and d to be private-key.

Procedure for Encryption of RSA

Abdul chooses P as a plain text.

Abdul calculates ciphertext as per the following method:

$$\text{Ciphertext}(C) = P^e \bmod(n)$$

Abdul sends ciphertext C to Waleed.

Procedure for Decryption of RSA

Waleed receives C as a ciphertext.

Waleed calculates P (Plain text) by using following method:

$$\mathrm{Plaintext\ (P) = C^{d}\ mod\ (n)}$$

5 Result Analysis of ECC and RSA

For analysis of RSA and ECC we have used the following parameter of RSA cryptography algorithm which recommended by NIST [10].

For elliptic curve cryptography the following equation is used:

E: $y^2 = x^3 - 3x + b$ (mod p). In this p is big (large) prime number.

Key length of 192 bits following parameters is used as shown below in Table 1.

Key length of 224 bits the following parameters is used as shown below in Table 2.

For 256, 384 and 512 bits key length of elliptic curve we have taken which in mentioned in [10].

For the encryption & decryption both algorithm RSA & ECC we have used the following plain text: “Our research focuses on comparative study of RSA and ECC”. Form comparing time analysis of we have used the same plain text for both algorithms [20, 21].

We found the required time to produce key for RSA and ECC using the suggested settings and in the provided configuration system, which are listed in the Table 3.

Table 1 Key length of 192 bits

$p =$	6277101735386680763835789423207666416083908700390324961279
$n =$	6277101735386680763835789423176059013767194773182842284081
$c =$	3099d2bbbfcb2538542dcd5fb078b6ef5f3d6fe2c745de65
$b =$	64210519 e59c80e70fa7e9ab72243049 feb8deec c146b9b1
$\mathrm{G_x} =$	188da80e b03090f67cbf20eb43a18800f4ff0afd82ff1012
$\mathrm{G_y} =$	07192b95ffc8da78631011ed6b24cdd573f977a11e794811

Table 2 Key length of 224 bits

$p =$	26959946667150639794667015087019630673557916260026308143510066298881
$n =$	26959946667150639794667015087019625940457807714424391721682722368061
$c =$	5b056c7e 11dd68f40469ee7f 3c7a7d74 f7d121116506d031218291fb
$b =$	b4050a85 0c04b3ab f54132565044b0b7d7bfd8ba270b39432355ffb4
$\mathrm{G_x} =$	b70e0cbd 6bb4bf7f 321390b94a03c1d3 56c21122343280d6115c1d21
$\mathrm{G_y} =$	bd376388 b5f723fb4c22dfe6 cd4375a05a07476444d5819985007e34

Table 3 Key generation time requirement

			Key Generation Required Average Time (Seconds)	
Security Bits	RSA	ECC	RSA	ECC
80	1536	192	1.3188	0.0904
112	2048	224	0.2752	0.1028
128	3072	256	6.3312	0.103
192	7680	384	29.5404	0.1188
256	15360	512	58.1994	0.1436

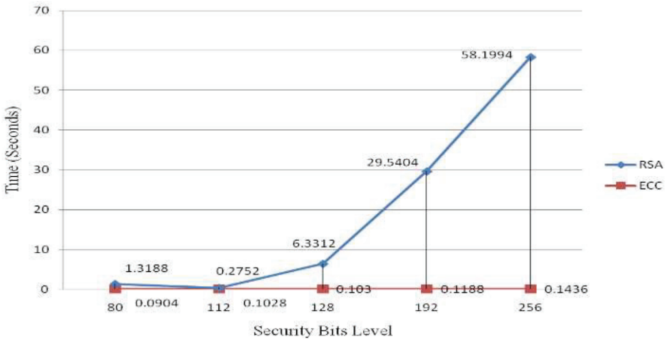

Figure 6 Performance of key generation vs. time.

5.1 Performance of Key Generation in Term of Time: ECC and RSA

Figure 6 depicts that from 80 to 112 bits what is time required to generate in RSA cryptographic is same elliptic cartographic but we want to achieve the security level 128 bits then time difference between this algorithm is more. It means that in RSA is required more time as compared to ECC. When we increase the bit size of security level time difference exponentials increases [22]. From Table 4, it is cleared that ECC is faster as compare to RSA to generate key of ECC and required.

5.2 Performance for Encryption in Term of Time: ECC and RSA

The above Figure 7 depicts, that the time taken by RSA algorithm for encryption is lesser than the one with ECC algorithm. It means that RSA algorithm is faster as In terms of encryption time, compared to the ECC Algorithm [23, 24]. From the results, we also analyzed the gap between

Table 4 Performance for encryption

SNO	Key Size of RSA	Key Size of ECC	RSA Time (Seconds)	ECC Time (Seconds)
1	1536	192	0.078	0.2062
2	2048	224	0.072	0.2096
3	3072	256	0.0812	0.2158
4	7680	384	0.0844	0.2282
5	15360	512	0.1	0.251

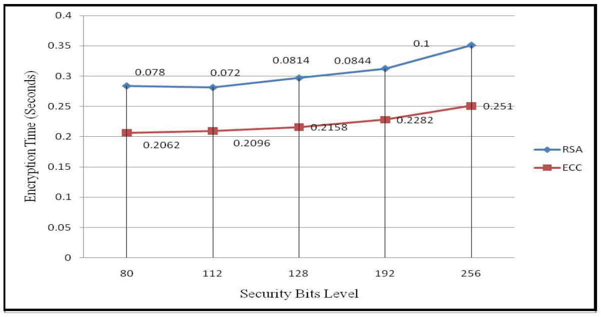

Figure 7 Performance for encryption.

Table 5 Performance for decryption

SNO	Size of Key RSA	Size of Key ECC	RSA Time (Seconds)	ECC Time (Seconds)
1	1536	192	0.0625	0.0525
2	2048	224	0.0782	0.0582
3	3072	256	0.0812	0.059
4	7680	384	0.1096	0.07
5	15360	512	0.2658	0.0811

the two computational times is not too much. In terms of encryption, we may infer that the two algorithms perform similarly, although the RSA-based technique outperforms the others in Tables 5 and 6.

The above Figure 8 depicts, that the time taken by ECC algorithm for decryption is much lesser than the one with RSA algorithm. It means that ECC algorithm is faster as compared to RSA Algorithm in terms of decryption time. We may conclude that the ECC algorithm outperforms the RSA approach in terms of decryption.

Data security is becoming increasingly important in today's digital world. Finding the best technique to keep one's data safe is a key worry for anyone.

Table 6 Performance for all three key generation, encryption & decryption

SNO	Bits of Security	RSA Key Generation + Encryption + Decryption	ECC Key Generation + Encryption + Decryption
1	80	1.459	0.3491
2	112	0.4254	0.3706
3	128	6.4938	0.3778
4	192	29.7344	0.417
5	256	58.5652	0.4757

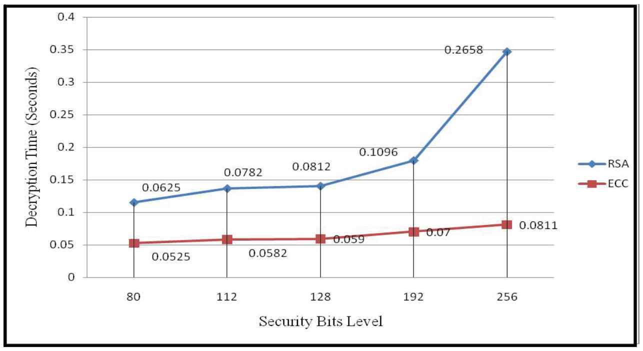

Figure 8 Performance for decryption.

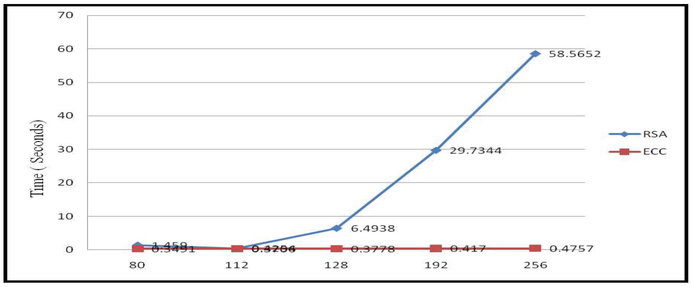

Figure 9 Performance for all three key generation, encryption & decryption.

For security, we have to focus on three main components: Time spent on key generation, encryption, and decryption.

As shown in above Table 6 depicts, that the combined time (Key Generation + Encryption + Decryption) taken by RSA and ECC algorithm. The cumulative time taken by RSA is substantially longer than the time taken by the ECC method. As a result, the ECC algorithm is more optimal and efficient than the RSA algorithm as shown in Figure 9.

6 Conclusion

In this paper, we compared RSA and ECC on the basis of various characteristics such as key generation, encryption, and decryption time, both independently and in combination. We observed that only in case of encryption, RSA is taking slightly less time in execution as compared to Elliptic curve cryptography. RSA algorithm is required exponential calculation for encryption & decryption but ECC algorithm (encryption & decryption) multiplication required it means less times required.

In case of key generation of different size of bits, ECC required less time (linear graph) as compare to RSA exponential graph. Result analysis also shows that ECC also consuming less time ass compare to RSA for decryption process. all three parameters (Key generation, encryption decryption) together it is found that ECC is much faster and efficient as compared to RSA algorithm.

The reason behind this comparison is that future generation will be based on smart devices like IoT. IoT has some constraints regarding size and processing speed. By using elliptic curve cryptography (ECC), this constraint of IoT can be minimized as ECC requires less key size for providing security.

The research paper provides a thorough evaluation of RSA and ECC cryptographic systems' performance for a range of key sizes and security levels. The study includes key generation, encryption, and decryption timings to assess each algorithm's effectiveness and applicability for various applications. The findings show that, compared to RSA, ECC has significant advantages, especially in terms of encryption and decryption processes. ECC is the best option in situations where speed is a crucial factor because it consistently displays better encryption and decryption speeds.

The study also demonstrates ECC's astounding key generation efficiency, beating RSA substantially at higher security settings. Because of this quality, ECC is especially well suited for memory-restricted devices like Palmtops, Smartphones, and Smartcards, where resource optimisation is essential. The data in the article also demonstrates a trade-off between performance and security level for both RSA and ECC. Encryption, decryption, and key generation times all grow as security level does with increasing key sizes. ECC, however, continues to outperform RSA in terms of performance even at higher security settings.

The research's conclusions indicate that ECC should be seriously taken into consideration for applications needing high-performance encryption without sacrificing security. For memory-constrained devices and situations where speed and effective key generation are crucial, it appears as a potential RSA substitute. The final decision between RSA and ECC should be made based on the demands and limitations of the intended application. The study offers insightful information on the actual applications of using RSA and ECC, assisting decision-makers in selecting the best cryptographic solution for their unique use cases.

Data availability statement: All data are made available in the manuscript.

Conflict of interest: The authors declare no conflict of interest.

Funding information: None.

References

[1] Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., and Ni, T. Y. 'A multi-dimensional adversary analysis of RSA and ECC in block chain encryption', In Future Information and Communication Conference Springer, Cham, pp. 988–1003. March. 2019.

[2] Rivest, R. L., Shamir, A., and Adleman, L. 'A method for obtaining digital signatures and public-key cryptosystems'. Communications of the ACM, vol. 212, pp. 120–12, 1978.

[3] Kumar, A., Tyagi, S. S., Rana, M., Aggarwal, N., and Bhadana, P. 'A comparativestudy of public key cryptosystem based on ECC and RSA'. International Journal on Computer Science and Engineering, vol. 35, pp. 1904–1909, 2011.

[4] Sethi, P. C., Sahu, N., and Behera, P. K. 'Group security using ECC'. International Journal of Information Technology, pp. 1–9, 2021.

[5] Sethi, P. C., and Behera, P. K. 'Network traffic management using dynamic bandwidth on demand'. International Journal of Computer Science and Information Security (IJCSIS), vol. 156, pp.369–375, 2017.

[6] Kumar, S., and Paar, C. Are standards compliant elliptic curve cryptosystems feasible on RFID. In Workshop on RFID security Citeseer, July, pp. 12–14, 2006.

[7] Bafandehkar, M., Yasin, S. M., Mahmod, R., and Hanapi, Z. 'Comparison of ECC and RSA algorithm in resource constrained devices'. International conference on IT convergence and security (ICITCS) December. pp. 1–3, 2013.

[8] Hankerson, D., Menezes, A. J., and Vanstone, S. 'Guide to elliptic curve cryptography. Springer Science & Business Media' 2006.

[9] Thiranant, N., Lee, Y. S., and Lee, H. 'Performance comparison between RSA and elliptic curve cryptography-based QR code authentication'. "2015" International Conference on Advanced Information Networking and Applications Workshops, pp. 278–282.

[10] Mallouli, F., Hellal, A., Saeed, N. S., and Alzahrani, F. A. 'A survey on Cryptography: comparative study between RSA vs ECC Algorithms,' and RSA vs El-Gamal algorithms. 2019.

[11] Fang, X., and Wu, Y. 'Investigation into the elliptic curve cryptography.' International Conference on Information Management (ICIM) IEEE, pp. 412–415.

[12] Mohammed Shuaib, Shadab Alam, Mohammad Shabbir Alam, Mohammad Shahnawaz Nasir. Compliance with HIPAA and GDPR in block chain-based electronic health record', Materials Today: Proceedings, pp. 2214–853, 2017.

[13] Mohammed Shuaib, Shadab Alam, Mohammad Shahnawaz Nasir, Mohammad Shabbir Alam. 'Immunity credentials using self-sovereign identity for combating COVID-19 pandemic', Materials Today: Proceedings, pp. 2214–7853. 2022.

[14] Mohammed Shuaib, Shadab Alam, Mohammad Shabbir Alam, Mohammad Shahnawaz Nasir. 'Self-sovereign identity for healthcare using blockchain', Materials Today: Proceedings, pp. 2214–7853, 2021. https://doi.org/10.1016/j.matpr.2021.03.083.

[15] Syed MH, Upreti K, Nasir MS, Alam MS, Kumar Sharma. 'Addressing image and Poisson noise deconvolution problem using deep learning approaches'. Computational Intelligence. pp. 1–15, 2022. doi: 10.1111/coin.12510.

[16] Kumar, N., Upreti, K., and Mohan, D. 'Blockchain Adoption for Provenance and Traceability in the Retail Food Supply Chain'. A Consumer Perspective. International Journal of E-Business Research (IJEBR), vol. 182, pp. 1–17. 2022. http://doi.org/10.4018/IJEBR.294110.

[17] Upreti K., Singh U.K., Jain R., Kaur K., Sharma A.K. 'Fuzzy Logic Based Support Vector Regression (SVR) Model for Software Cost Estimation Using Machine Learning'. In: Tuba M., Akashe S., Joshi A. (eds) ICT Systems and Sustainability. Lecture Notes in Networks and Systems, vol 321. Springer, Singapore, 2022. https://doi.org/10.1007/978-981-16-5987-4_90.

[18] Upreti K., Kumar V., Pal D., Alam M.S., Sharma A.K. 'Design and Development of Tracking System in Communication for Wireless Networking'. In: Nagar A.K., Jat D.S., Marín-Raventós G., Mishra D.K. (eds) Intelligent Sustainable Systems. Lecture Notes in Networks and Systems, vol. 334, 2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-6369-7_19.

[19] K. Upreti, A. Verma, R. Jain and Y. Bekuma. 'Broadcasting Scheme for Real Time Video in mobile Adhoc Network'. Turkish Journal of Computer and Mathematics Education, vol. 1211, pp. 3799–3803, 2021.

[20] Palanikkumar, D., Upreti, K., Venkatraman, S., Suganthi, J. R., Kannan, S. et al. 'Fuzzy Logic for Underground Mining Method Selection. Intelligent Automation & Soft Computing, vol. 323, pp. 1843–1854, 2021.

[21] Kumar N., Singh M., Upreti K., and Mohan D. Block chain Adoption Intention in Higher Education: Role of Trust, Perceived Security and Privacy in Technology Adoption Model. In: Proceedings of International Conference on Emerging Technologies and Intelligent Systems. vol. 299. 2022. https://doi.org/10.1007/978-3-030-82616-1_27.

[22] Upreti K., Kumar V., Pal D., Alam M.S., Sharma A.K. 'Design and Development of Tracking System in Communication for Wireless Networking'. In: Intelligent Sustainable Systems. vol. 334, 2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-6369-7_19.

[23] Kumar, N., Upreti, K., Upreti, S., Shabbir Alam, M., and Agrawal, M. 2021, Blockchain integrated flexible vaccine supply chain architecture: Excavate the determinants of adoption.' Human Behavior and Emerging Technologies, 1–12, 2021. https://doi.org/10.1002/hbe2.302.

[24] A.K. Sharma, Kamal Upreti, Binu Vargis. 'Experimental performance analysis of load balancing of tasks using honey bee inspired algorithm for resource allocation in cloud environment', Materials Today: Proceedings, pp. 2214–7853. 2022.

[25] A. Sharma, U. K. Singh, K. Upreti, N. Kumar and S. K. Singh, A Comparative analysis of security issues & vulnerabilities of leading Cloud Service Providers and in-house University Cloud platform for hosting E-Educational applications. IEEE Mysore Sub Section International Conference (MysuruCon), pp. 552–560. 2021. doi: 10.1109/MysuruCon52639.2021.9641545.

[26] A. Sharma, U. K. Singh, K. Upreti and D. S. Yadav. 'An investigation of security risk & taxonomy of Cloud Computing environment,' 2nd International Conference on Smart Electronics and Communication

(ICOSEC), pp. 1056–1063, 2021. doi: 10.1109/ICOSEC51865.2021.9591954.

[27] K. Upreti, B. K. Vargis, R. Jain and M. Upadhyaya. 'Analytical Study on Performance of Cloud Computing with Respect to Data Security,' 5th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 96–101, 2021. doi: 10.1109/ICICCS51141.2021.9432268.

[28] Kamal Upreti, A.K. Sharma, Binu Vargis, Rajwinder Singh Sidhu. 'An efficient approach for generating IRIS codes for optimally recognizing IRIS using multi objective genetic algorithm,' Materials Today: Proceedings, pp. 2214–7853, 2022. https://doi.org/10.1016/j.matpr.2020.10.085.

[29] Kamal Upreti, Mohammad Shahnawaz Nasir, Mohammad Shabbir Alam, Ankit Verma, A.K. Sharma. 'Analyzing real time performance in Vigil Net using Wireless Sensor Network,' Materials Today: Proceedings, pp. 2214–7853, 2021. https://doi.org/10.1016/j.matpr.2021.01.490.

[30] Bao, Jiaxu. "Research on the security of elliptic curve cryptography." 2022 7th International Conference on Social Sciences and Economic Development (ICSSED 2022). Atlantis Press, 2022.

[31] Ullah, Shamsher, et al. "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey." Computer Science Review 47 (2023): 100530.

[32] D. Boneh and H. Shacham, "Fast variants of RSA," CryptoBytes, vol. 5, no. 1, pp. 1–9, 2002.

[33] C. C. Chang and M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems," Electronics Letters, vol. 32, no. 15, pp. 1365–1366, 1996.

[34] P. Verma, D. Mahto, S. K. Jha and D. K. Yadav, "Efficient RSA cryptosystem with key generation using matrix," International Journal of Control Theory and Applications, vol. 10, no. 13, pp. 221–228, 2017.

[35] A. Mansour, A. Davis, M. Wagner, R. Bassous, H. Fu and Y. Zhu, "Multi-asymmetric cryptographic RSA scheme," in Proceedings of the 12th Annual Conference on Cyber and Information Security Research, p. 9, 2017.

[36] K. R. Santosh, C. Narasimham and P. Shetty, "Cryptanalysis of multiprime RSA with two decryption exponents," International Journal of Electronics and Information Engineering, vol. 4, no. 1, pp. 40–44, 2016.

[37] X. D. Dong, “A multi-secret sharing scheme based on the crt and RSA,” International Journal of Electronics and Information Engineering, vol. 2, no. 1, pp. 47–51, 2015.

[38] A. Takayasu and N. Kunihiro, “General bounds for small inverse problems and its applications to multiprime RSA,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 100, no. 1, pp. 50–61, 2017.

[39] K. Bhardwaj and S. Chaudhary, “Implementation of elliptic curve cryptography in c,” International Journal on Emerging Technologies, vol. 3, no. 2, pp. 38–51, 2012.

[40] Q. Qian, Y-L Jia and R. Zhang, “A lightweight rfid security protocol based on elliptic curve crytography,” International Journal Network Security, vol. 18, no. 2, pp. 354–361, 2016.

[41] S. Basu, “A new parallel window-based implementation of the elliptic curve point multiplication in multi-core architectures,” Group, vol. 14, pp. 101–108, 2012.

[42] M. S. Srinath and V. Chandrasekaran, “Isogenybased quantum-resistant undeniable blind signature scheme,” International Journal of Network Security, vol. 20, no. 1, pp. 8–17, 2018.

[43] Saho, Nelson Josias Gbètoho and Eugène C. Ezin. “Comparative Study on the Performance of Elliptic Curve Cryptography Algorithms with Cryptography through RSA Algorithm.” (2020).

Biographies

Mohammad Rafeek Khan is currently working a Lecturer with the Department of Computer and Network Engineering, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia. He received his MCA degree from Aligarh Muslim University, Aligarh, India in 2007. He has published many articles in reputed journals. His research interests include Cryptographic Techniques & Security, Machine Learning and computer vision.

Kamal Upreti is currently working as an Associate Professor in Department of Computer Science, CHRIST (Deemed to be University), Delhi NCR, Ghaziabad, India. He completed is B. Tech (Hons) Degree from UPTU, M. Tech (Gold Medalist) from Galgotias University, PGDM (Executive) from IMT Ghaziabad and PhD from OPJ University in Department of Computer Science & Engineering. Now, he is doing Postdoc from National Taipei University of Business, TAIWAN funded by MHRD.

He has published 50+ Patents, 35+ Books, 32+ Magazine issues and 70+ Research papers in in various international Conferences and reputed Journals. His areas of Interest are Cyber Security, Machine Learning, Health Care, Wireless Networking, Embedded System and Cloud Computing.

Mohammad Imran Alam is currently working a Lecturer with the Department of Computer and Network Engineering, College of Computer Science and Information Technology, Jazan University, Jazan, Saudi Arabia.

He received his MCA degree from Aligarh Muslim University, Aligarh, India in 2007. He has published many articles in reputed journals. He has more than 15 years of teaching experience. His research interests include Cryptographic Techniques, Block Chain, IoT and Machine Learning.

Haneef Khan has been working as an Lecturer in the Department of Computer and Network Engineering, Jazan University, Jazan, KS. He has received the B.Tech. degree in electronics from UPTU, in 2008, and the M.Tech. degree in electronics from MDU, in 2012. He has more than 12 years of teaching experience. He has also undertaken funded projects as a principal investigator. His research interests include the Internet of Things, device-to-device communication, and blockchain.

Shams Tabrez Siddiqui currently working as an Assistant Professor in the Department of Computer Science, Jazan University, Jazan, KSA. He received his PhD and MCA degree from Aligarh Muslim University, Aligarh, India in 2015 and 2007. He has worked as a counsellor for IGNOU. He has published more than 50 research papers in different reputed international/national journals, conference proceedings and book chapters. His research interest includes Software Requirement Engineering, Software Engineering and

Software Security. He extended his research area to IoT, Wireless Sensor Networks, Cloud Computing and Blockchain. He is a member of the Computer Society of India, IAENG, ACM, IAENG, CSTA, ICSES and IACSIT. He worked as a reviewer for many journals.

Mustafizul Haque, Associate Professor of Marketing Management, Dr. D.Y. Patil Vidyapeeth's Centre for Online Learning, Dr. D.Y. Patil Vidyapeeth, Pune (Deemed to be University). I obtain B.com (2008) from Patna University, Patna, M.B.A (2010) from G.B.T.U, Lucknow, Doctoral Degree in 2015 Faculty of Management from B.R.A.B.U Muzaffarpur, Bihar, M.Com from MATS University, Raipur in (2018) and M.B.A (Fire & Safety Management) from National Institute of Fire & Safety Engineering, Nagpur in (2021). He has served as faculty member such as M.S college, Motihari; I.T.M, Aligarh; Aurora PG College (MBA), Hyderabad and G H Rai Soni University (M.P). He has contributed more than 40 Paper in SCI, ABDC, Springer, Scopus Index, National, International journals, Conferences, Seminars, FDP, MOUs and Ten Text Book Published and Eight Patent.

Jyoti Parashar is currently working as an Assistant Professor in Department of Computer Science & Engineering, Dr. Akhilesh Das Gupta Institute of

Technology & Management (Formerly NIEC) affiliated to Guru Govind Singh Indraprastha University, Delhi, India. She has published Patents, Books, Magazine issues and Research papers in various international Conferences and reputed Journals. Her areas of Interest are Machine Learning, Health Care, Wireless, Cloud Computing, Internet of Things, Big Data, Ad Hoc Network and Internet security. She is having enriched years' experience in corporate and teaching experience in Engineering Colleges.