JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Performance Evaluation of Cryptography Algorithms: AES, DES, RSA, and ECC

[1]Komal, [2]Naveen Kumar, [3]Sandeep Kumar, [4]Ashok Kumar Kashyap, [5]Ritesh Rana
[1,5]Research Scholar, [2,3,4] Assistant Professor
[1]Department of Computer Science
[1]Himachal Pradesh University, Summerhill, Shimla

Abstract: In the modern era of digitization everything is evolving gradually and meeting new requirements in terms of data and information. This can lead to the transformation of data and the modernization of information. For data transformation, it is necessary to secure the data as data theft and information vulnerability are growing every day. To protect data and information many aspects are taken as security which can be provided by cryptography. It secures data by exchanging public and private keys for sending and receiving the data, so only authorized users can receive or access the data. In modern times, cryptography applications have emerged in new ways for the development process. Cryptography ensures that the information or data can be protected against malicious attacks. In this paper various symmetric and asymmetric cryptography algorithms AES, DES, RSA, and ECC respectively are analyzed for performance and security. The performance is measured on execution time, CPU speed, and memory requirements. The analysis is performed on the cryptography algorithms and based on this comparative tables are designed according to the selected parameters which give the efficiency of the individual algorithm demonstrated in the graph.

Keywords: AES, DES, RSA, ECC, Encryption, Decryption.

I. Introduction

Cryptography protects data and information over a network from threats, unauthorized access, and breaches. This is a vast term that describes hardware and software solutions relating to threat protection. It is an emerging technique that prevents the theft of data and provides safe data transfer between the initiator and receiver. A secret key is used for encrypting the data which can only be retrieved by intended users. Cryptography has many applications, including smart cards, passwords, e-commerce, smart homes, etc.

In this paper, cryptography algorithms are chosen and tested for their performance on the parameters such as execution time, encryption time, throughput, and decryption time. Implementation of software aids in minimizing the processor and memory requirements. Google Colab has been chosen as the implementation tool and Google cloud for data transformation. Cryptography algorithms can be divided into various categories, and finding an algorithm that requires fewer resources and provides secure communication is a difficult task. The main focus of the paper is:

a. Providing the comparison of cryptography algorithms using Google Colaboratory based on the python programming language. The algorithms' implementation is based on parameters like encryption time, decryption time, throughput, and total time.
b. Analyze the output of software implementations and arrange the algorithms according to evaluation metrics.
c. Select the algorithm that performs most efficiently in all performance metrics.

The following are the remaining sections of the paper: Section 2 discusses cryptography algorithms. Section 3 describes previous work done by other researchers. Section 4 compares the performance of cryptography algorithms implemented in Google Colab and discusses the results. Section 5 provides the conclusion.

II. Cryptography

Cryptography is a technique used for the conversion of plain text into cipher text for providing the security of data and information on different devices [1]. Cryptography includes various techniques like word-image fusion and other methods for providing secure data transmission. It is the study of techniques for secure communication in the presence of attackers.
Modern cryptography concerns itself with the following objectives [2]:

a. **Confidentiality:** Securing the data so that no other person other than the intended user can understand the data [3].
b. **Integrity:** The data can't be modified or accessed by the unauthorized user without being noticed when it is in transit or storage [4].
c. **Non-repudiation**: The sender has to bear the responsibility for the data transmitted so that in the later stages he/she can't deny it [5].
d. **Authentication:** The identity of the sender and receiver has to be confirmed by each other [6].

2.1 Cryptography Algorithms Considered for Evaluation

2.1.1 Advanced Encryption Standard (AES)

AES is the symmetric encryption algorithm based on the Substitution Permutation Network (SPN) structure [7]. It is a symmetric encryption standard used for secure data transfer between the initiator and receiver [8]. It is a block cipher consisting of different key lengths 2^7 bits, 192 bits, and 2^8 bits. It contains four basic tasks: Sub Bytes, Shift Rows, Columns, and Round key [9].

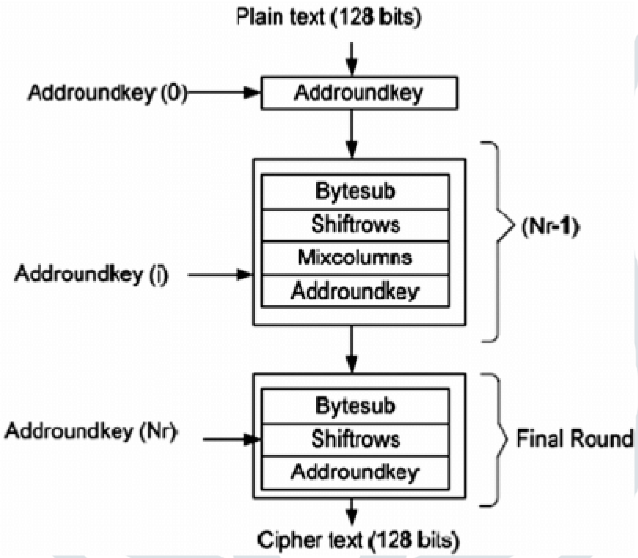


Fig1.1 AES Encryption Algorithm Structure [10].

2.1.2 DATA ENCRYPTION STANDARD (DES)

It is a block cipher based on SKE [11]. At the encryption site, DES generates a 64-bit ciphertext from a 64-bit plaintext, and at the decryption site, DES generates a 64-bit block of plaintext from a 64-bit ciphertext. Both encryption and decryption use the same 56-bit cipher key. The DES network is based on the Feistel network (FN). The algorithm is strengthened throughout 16 rounds. DES was built for hardware; it is fast in hardware but only moderately fast in software [12].

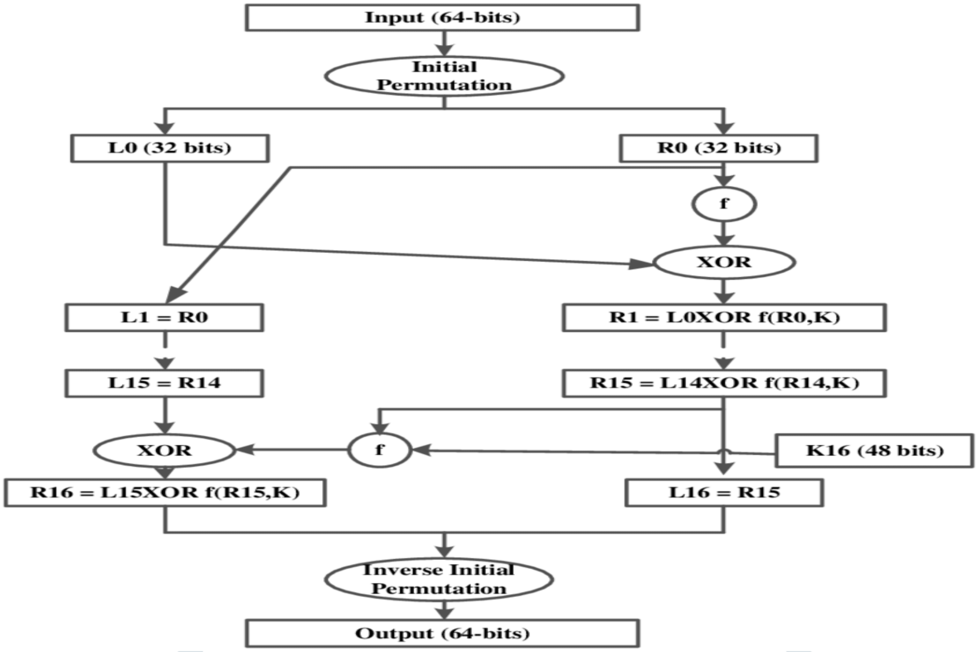
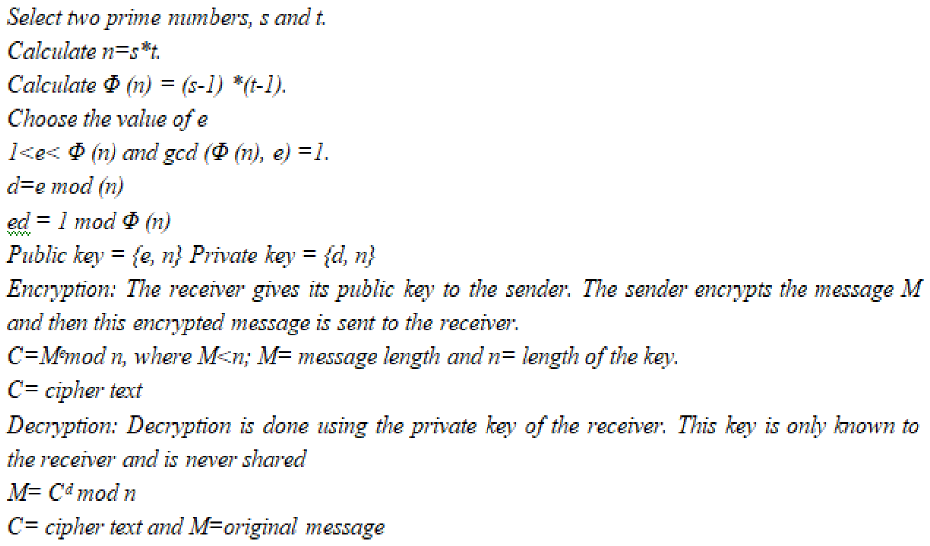


Fig 1.2 Structure of DES Encryption Algorithm [13].

2.1.3 Rivest Shamir Adlmen (RSA)

RSA is considered the most secure way of encryption. RSA uses prime numbers and exponents. The integers used in this method are quite large making it difficult to decrypt. Here we use 2 keys i.e., public and private. RSA is used in SSL, MIME, RSA signature, and verification. The key distribution problem is solved in RSA and it removes the problem of authentication and confidentiality that we had in symmetric key cryptography [14]. RSA provides us with digital signatures so that no unauthorized user can tamper with the data. The public key used in RSA is shared over the network but the private key is not shareable [15]. Data in RSA cannot be modified. RSA is used with DSA to solve the problem of authentication and integrity of the message. RSA keys are mainly 2^{10} to 2^{11} bits and increasing the key size increases the encryption strength exponentially. Key generation is slow in RSA and the algorithm fails if the message length is greater than the key size [16].

RSA ALGORITHM



Select two prime numbers, s and t.
*Calculate n=s*t.*
*Calculate Φ (n) = (s-1) *(t-1).*
Choose the value of e
1<e< Φ (n) and gcd (Φ (n), e) =1.
d=e mod (n)
ed = 1 mod Φ (n)
Public key = {e, n} Private key = {d, n}
Encryption: The receiver gives its public key to the sender. The sender encrypts the message M and then this encrypted message is sent to the receiver.
C=M^emod n, where M<n; M= message length and n= length of the key.
C= cipher text
Decryption: Decryption is done using the private key of the receiver. This key is only known to the receiver and is never shared
M= C^d mod n
C= cipher text and M=original message

Fig 1.3 RSA Algorithms [17].

2.1.4 Elliptic Curve Cryptography (ECC)

ECC is gaining a lot of popularity as an alternative to RSA. ECC is a PKC based on an elliptic curve. It gives us faster, smaller, and more efficient cryptography keys using the elliptical curve equation. ECC generates keys that are mathematically harder to decrypt. ECC keys are harder to decrypt since they are very difficult to generate as well as decode [18].

Victor Miller and Neil Koblitz discovered ECC in 1985. Security in ECC is obtained from an elliptic curve logarithm. In constrained devices like mobile phones and wireless devices having limited bandwidth, memory, and battery life a public key cryptosystem must be chosen so that it is efficient in terms of Computing cost, storage cost, and key size [19]. ECC provides the highest security per bit as compared to other cryptography algorithms. Smaller key size helps to reduce and save bandwidth memory and processing power. RSA having 1024 bits is equivalent to 256-bit ECC in terms of security. ECC keys are difficult to break. Cryptographic resistance per bit in ECC is much greater than other cryptography algorithms present, it requires lesser memory storage, has greater encryption and signing speed in both hardware and software implementation, and is also ideal for small-size hardware implementation [20].

PROPERTIES OF ELLIPTIC CURVE

- The elliptic curve is symmetric along the x-axis.
- If we draw a line through the curve, it will touch a maximum of 3 points.

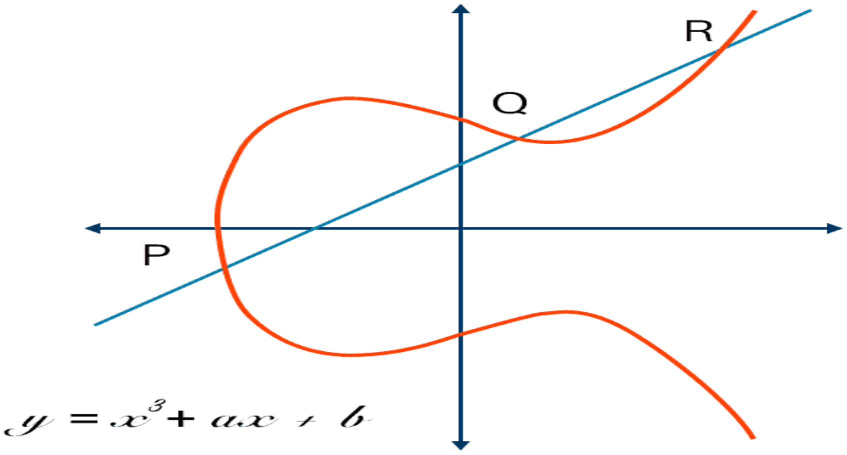


Fig. 1.3: Elliptic Curve used in ECC [21].

III. Related Work

All the work mentioned below has been done by the researcher earlier and distinguishes the different algorithms and depicts the algorithm gives the satisfactory result: -

DSA Minaam et al. The work gives the efficiency of symmetric algorithms like AES, DES, 3DES, RC6, Blowfish, and RC2. Comparison has been taken for every individual algorithm at varying environment setups such as a variety of data blocks, unique datatypes, consumption of power, varying size of the key, and the speed in which the encryption/decryption is taken. From the above algorithms, it is found that the AES gives better outcomes, is faster, and is very efficient [22].

NA Al-gohany and S Almotairi presented a comparative study between AES and DES regarding varying input (KB) and the same key size. The Outcomes show that AES is more efficient and much faster than DES. So, it is better to use this for securing the data in the cloud [23].

Nivedita Bisht and Sapna Singh compared different factors of both key encryption algorithms like AES, DES, RSA, and DIFFIE-HELLMAN. It is analyzed that AES is best in security, accuracy, speed of cryptography, and power consumption in symmetric encryption. RSA is best in security and speed in asymmetric key encryption [24].

Nishant Agnihotri and Aman Kumar Sharma compared five different techniques of symmetric cryptography such as AES, IDEA, RC6, TwoFish, and MARS on three different strings. These algorithms are used to encode and decode the plain and cipher text. All these are compared based on their memory requirements and the time taken to perform encryption. AES takes minimum time for encrypting and decrypting data, so it is found to be the most efficient technique [25].

B. Mandal et al. compared some of the traditional algorithms AES, DES, 3DES, and Blowfish and it is found that Blowfish is highly recommended to give better outcomes for encryption. Symmetric key cryptography gives security to various fields like WSN, MANET, VANET, etc. In terms of the primary requirement of security, it is proved that Symmetric Key Cryptography is more efficient in software and AES is better in both Software and Hardware. This is the most suitable and most used method in the proposed work because of its efficiency and outcomes [26].

S. Chandra et al. describe the traditional algorithms and the proposed algorithms based on their advantages and limitations, related to both key cryptographies. The outcomes discuss that proposed algorithms are highly efficient in their fields but there are some areas left for research work. The paper also discusses appropriate future work related to the proposed work. In the case of public key cryptography, the digital signature provides better functionality in sense of security [27].

J. D. Gaur et al. explained cryptography algorithms such as TwoFish, Blowfish, AES, IDEA, MD5, HMAC, RSA, and DES. On comparing these algorithms, it was shown that the blowfish algorithm works well for memory consumption and time utilization. Also, AES algorithms are chosen to prevent attacks and can be implemented on all Internet protocols based on IPv4 and IPv6. RSA algorithm remains one of the best algorithms that can be used for securing data with at most security [28].

S. Al Busafi and B. Kumar give an analysis of the different encryption techniques like RSA, Diffie-Hellman, Digital Signature, ECC, AES, and Blowfish. It tells about the way of using digital signatures which provides all primary requirements of security [29].

As per the literature, review work has been done by various researchers which demonstrates that security is of major concern for any device connected to the Internet. Hence, cryptography algorithms give better security for sending and receiving data or information from one place to another place. So, the objectives of the proposed work are: (i) To study and analyze symmetric and Asymmetric cryptographic algorithms, (ii) To implement AES, DES, RSA, and ECC in the Google Colaboratory environment, and (iii) To compare the cryptographic algorithms on the basis for performance evaluation.

IV. Tools Implementation and Simulation Setup

The simulation was performed using Python in Google collaborator. The system configuration included an Intel (R) core (TM) i5-7200Uprocessor with 2.50GHz CPU capacity with 4GB primary memory. The window 10 OS was employed for experimentation purposes. The experiment was done on 4 algorithms out of which 2 are symmetric and 2 are asymmetric and evaluation was done on these algorithms.

4.1 Results and Analysis

The result is concluded on the performance evaluation of time of encryption, decryption, execution, and throughput which are described below:

a. **Encrypting time:** The time taken in the process of converting ciphertext into plaintext with the appropriate encryption method.

b. **Decrypting time:** The time taken in the process of converting plaintext into ciphertext with the appropriate decryption method.

c. **Throughput:** It is the division of encrypted plaintext to encryption time. For the scheme of encryption, throughput is how fast the encryption is done. When it increases, power consumption decreases [30].

Table 1.1 Symmetric Cryptographic Algorithms

Symmetric Algorithms							
Algorithms	**Key Size (bits)**	**Encrypting Time (ms)**	**Decrypting Time (ms)**	**Total Time taken(ms)**	**Throughput(byte/ms)**	**CPU Speed (%)**	**Memory Requirement (%)**
DES	56-bits	525	548	1073	13.33	5.4	7.7
AES	128-bits	408	525	933	78.4	5.0	7.6

From the results of Table 1.1, it can be concluded that AES provides lesser encrypting and decrypting time as compared to DES. Memory requirement in AES is lesser in AES as compared to DES. Hence it is concluded that AES outperforms DES.

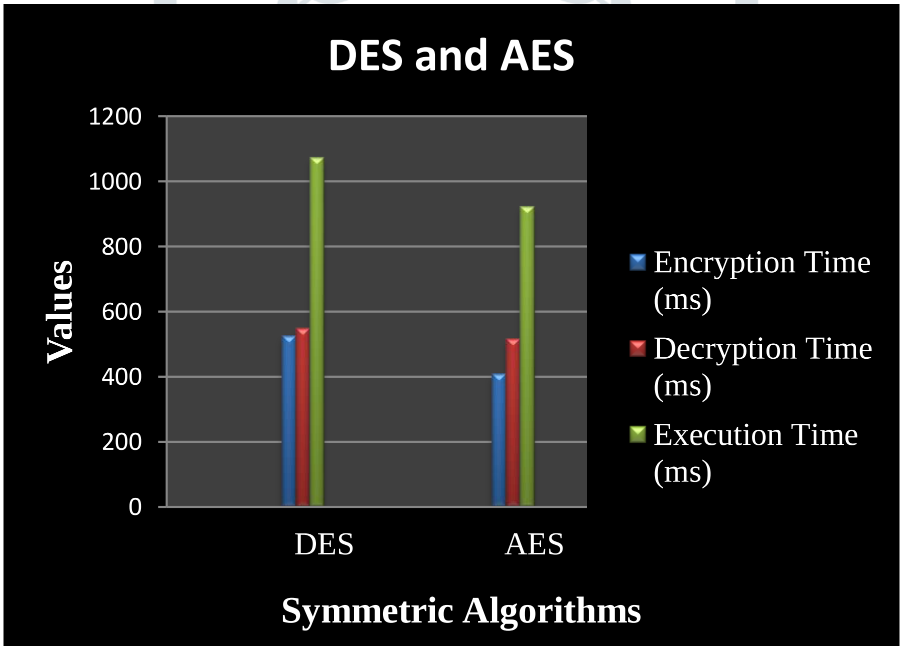


Fig 1.4:- Symmetric Algorithms

Fig 1.4 shows comparison between symmetric algorithms AES and DES. It depicts that AES outperforms DES in encrypting and decrypting data. For the security of data AES is recommended as it process in less time.

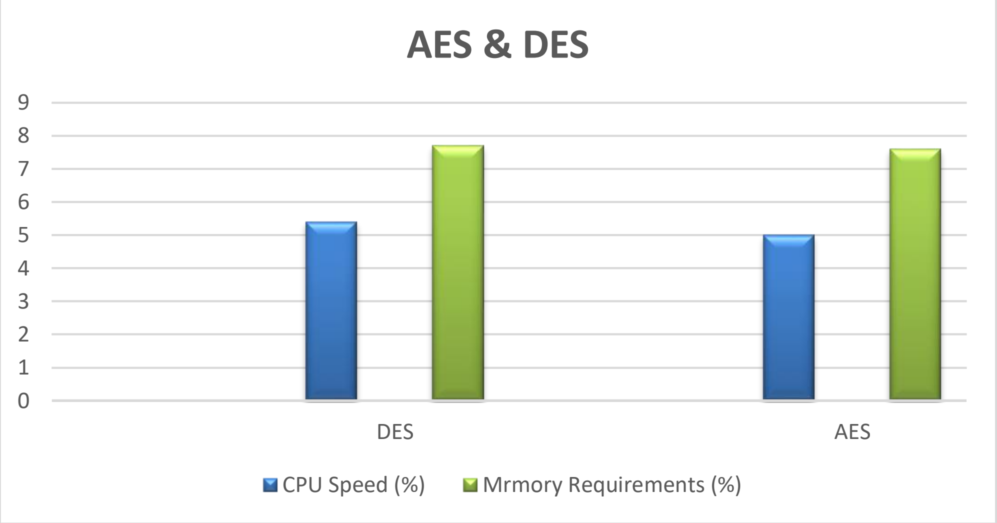


Fig 1.5:- AES and DES

The AES requires less memory as compared with DES. Hence AES outperforms DES.

Table 1.2 Asymmetric Cryptographic Algorithms

Asymmetric Algorithms						
Algorithms	**Key-Size (bits)**	**Encryption Key Time (s)**	**Decryption Key Time (s)**	**Total Time (s)**	**CPU Speed (%)**	**Memory Requirement (%)**
RSA	256-bits	939	608	1.547	6.5	7.8
ECC	256-bits	550	542	1.092	2.4	7.5

From the results of Table 1.2, it is concluded that ECC provides lesser encryption and decryption key time as compared to RSA.ECC has less memory requirement than RSA after being analyzed. It shows that ECC is a highly efficient algorithm for providing security.

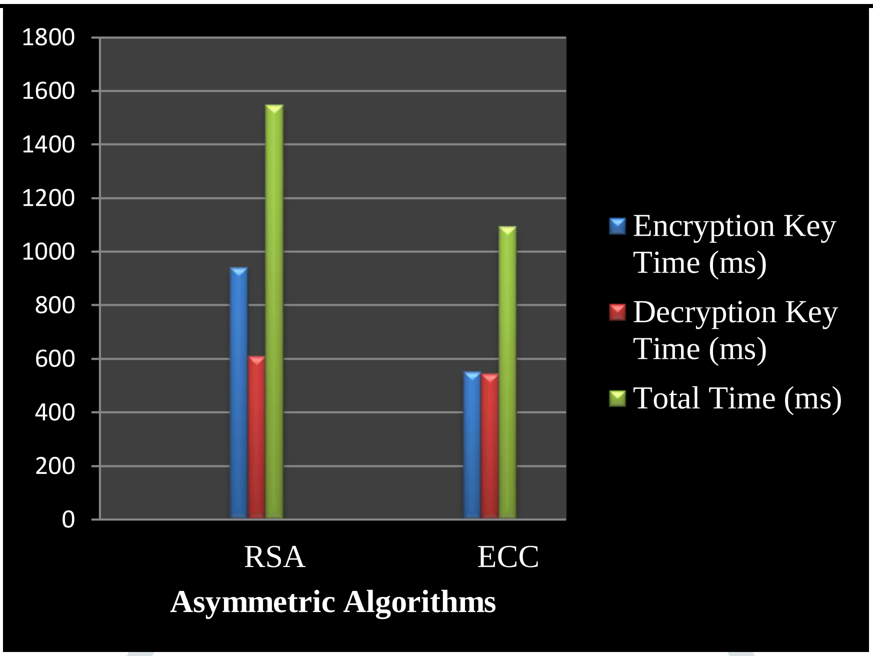


Fig 1.6:- Asymmetric Algorithms

Fig 1.5 shows a comparison between Asymmetric algorithms RSA and ECC. It depicts that ECC outperforms RSA in encrypting and decrypting keys.

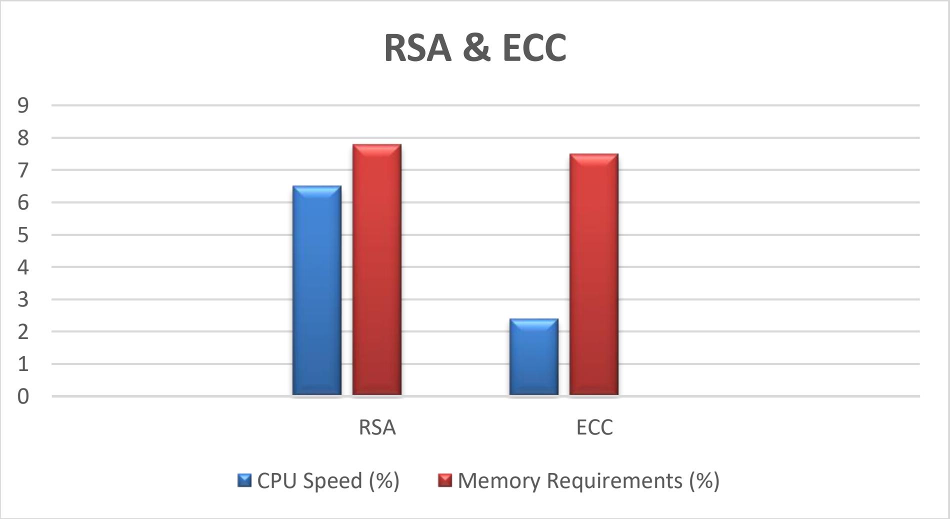


Fig 1.7:- RSA & ECC

The ECC requires less memory as compared with RSA. Hence ECC secures data more efficiently.

V. Conclusion

With the excessive growth of the Internet, data security becomes a serious concern for any individual or organization. The security of data is highly important as it can be of high risk, if not taken into consideration. Cryptography algorithms are getting versatile and involve private keys for encryption which provide secure transmission of data. The schemes used for cryptography are symmetric and asymmetric. The former can be used with the help of DES and AES. From the above results, it is clear that AES provides more security as compared to DES as it has lower encryption and decryption time. AES also has lesser memory requirements as compared to DES. ECC provides better results than RSA which makes it a more secure and reliable algorithm. It can be concluded that AES outperforms other cryptography algorithms and can be used for applications that require lesser time to encrypt the data. From the above results achieved; AES provides better security in terms of performance analysis. For future work, AES can be used to further reduce the execution time for better outcomes.

References:

[1] H. R. Pawar and D. G. Harkut, "Classical and Quantum Cryptography for Image Encryption & Decryption," 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), 2018, pp. 1-4, doi: 10.1109/RICE.2018.8509035.

[2] Aiden A. Bruen; Mario A. Forcinito; James M. McQuillan, "The Fundamentals of Modern Cryptography," in Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century , Wiley, 2021, pp.83-108, doi: 10.1002/9781119582397.ch4.

[3] C. Biswas, U. D. Gupta and M. M. Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019, pp. 1-5, doi: 10.1109/ECACE.2019.8679136.

[4] L. Krithikashree, S. Manisha and M. Sujithra, "Audit Cloud: Ensuring Data Integrity for Mobile Devices in Cloud Storage," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-5, doi: 10.1109/ICCCNT.2018.8493963.

[5] J. Choi, I. Shin, J. Seo and C. Lee, "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service," 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, 2011, pp. 331-333, doi: 10.1109/CNSI.2011.28.

[6] V. Venukumar and V. Pathari, "Multi-factor authentication using threshold cryptography," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 1694-1698, doi: 10.1109/ICACCI.2016.7732291.

[7] Fang Rao and Jianjun Tan, "Energy consumption research of AES encryption algorithm in ZigBee," International Conference on Cyberspace Technology (CCT 2014), 2014, pp. 1-6, doi: 10.1049/cp.2014.1330.

[8] Ritambhara, A. Gupta and M. Jaiswal, "An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT)," 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017, pp. 422-427, doi: 10.1109/CCAA.2017.8229877.

[9] L. Yu, D. Zhang, L. Wu, S. Xie, D. Su and X. Wang, "AES Design Improvements Towards Information Security Considering Scan Attack," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 322-326, doi: 10.1109/TrustCom/BigDataSE.2018.00056.

[10] Hua Li and Z. Friggstad, "An efficient architecture for the AES mix columns operation," 2005 IEEE International Symposium on Circuits and Systems (ISCAS), 2005, pp. 4637-4640 Vol. 5, doi: 10.1109/ISCAS.2005.1465666.

[11] Z. Yingbing and L. Yongzhen, "The design and implementation of a symmetric encryption algorithm based on DES," 2014 IEEE 5th International Conference on Software Engineering and Service Science, 2014, pp. 517-520, doi: 10.1109/ICSESS.2014.6933619.

[12] W. Yihan and L. Yongzhen, "Improved Design of DES Algorithm Based on Symmetric Encryption Algorithm," 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA), 2021, pp. 220-223, doi: 10.1109/ICPECA51329.2021.9362619.

[13] Enhancing Cryptographic Security based on AES and DNA Computing تعزيز التشفير الأمني أستناداً على معيار التشفير المتقدم و حوسبة الحمض النووي - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/A-Flowchart-of-DES-Algorithm-31_fig5_339999643 [accessed 21 Dec, 2022]

[14] Yunfei Li, Qing Liu and Tong Li, "Design and implementation of an improved RSA algorithm," 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT), 2010, pp. 390-393, doi: 10.1109/EDT.2010.5496553.

[15] Jizhong Liu and Jinming Dong, "Design and implementation of an efficient RSA crypto-processor," 2010 IEEE International Conference on Progress in Informatics and Computing, 2010, pp. 368-372, doi: 10.1109/PIC.2010.5687968.

[16] S. A. Nagar and S. Alshamma, "High-speed implementation of RSA algorithm with modified keys exchange," 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012, pp. 639-642, doi: 10.1109/SETIT.2012.6481987.

[17] M. Rahman, I. R. Rokon and M. Rahman, "Efficient hardware implementation of RSA cryptography," 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, 2009, pp. 316-319, doi: 10.1109/ICASID.2009.5276895.

[18] D. Xu and W. Chen, "3G communication encryption algorithm based on ECC-ElGamal," 2010 2nd International Conference on Signal Processing Systems, 2010, pp. V3-291-V3-293, doi: 10.1109/ICSPS.2010.5555894.

[19] K. Ravikumar and A. Udhayakumar, "Secure Multiparty Electronic Payments Using ECC Algorithm: A Comparative Study," 2014 World Congress on Computing and Communication Technologies, 2014, pp. 132-136, doi: 10.1109/WCCCT.2014.31.

[20] Güneysu, T., Paar, C. (2008). Ultra High Performance ECC over NIST Primes on Commercial FPGAs. In: Oswald, E., Rohatgi, P. (eds) Cryptographic Hardware and Embedded Systems – CHES 2008. CHES 2008. Lecture Notes in Computer Science, vol 5154. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-85053-3_5

[21] Elliptic Curve Cryptography. (2022). Retrieved December 21, 2022, from AVI Networks: https://avinetworks.com/glossary/elliptic-curve-cryptography/

[22] Minaam, D. S. A., Abdual-Kader, H. M., & Hadhoud, M. M. (2010). Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types. Int. J. Netw. Secure., 11(2), 78-87.

[23] Al-gohany, N. A., & Almotairi, S. (2019). Comparative study of database security in cloud computing using AES and DES encryption algorithms. Journal of Information Security and Cybercrimes Research, 2(1), 102-109.

[24] Bisht, N., & Singh, S. (2015). A comparative study of some symmetric and asymmetric key cryptography algorithms. International Journal of Innovative Research in Science, Engineering and Technology, 4(3), 1028-1031.

[25] N. Agnihotri and A. K. Sharma, "Comparative Analysis of Different Symmetric Encryption Techniques Based on Computation Time," 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 6-9, doi: 10.1109/PDGC50313.2020.9315848.

[26] B. Mandal, S. Chandra, S. S. Alam and S. S. Patra, "A comparative and analytical study on symmetric key cryptography," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014, pp. 131-136, doi: 10.1109/ICECCE.2014.7086646.

[27] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014, pp. 83-93, doi: 10.1109/ICECCE.2014.7086640.

[28] J. D. Gaur, A. Kumar Singh, N. P. Singh and G. Rajan V, "Comparative Study on Different Encryption and Decryption Algorithm," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2021, pp. 903-908, doi: 10.1109/ICACITE51222.2021.9404734.

[29] S. Al Busafi and B. Kumar, "Review and Analysis of Cryptography Techniques," 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 323-327, doi: 10.1109/SMART50582.2020.9336792.

[30] Ramesh, A., & Suruliandi, A. (2013, March). Performance analysis of encryption algorithms for Information Security. In 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT) (pp. 840-844). IEEE.