A Comprehensive Literature Review of Asymmetric Key Cryptography Algorithms

Vaishali Kanwar[1], Aman Sharma[2]
[1, 2] Dept of Computer Science
[1, 2] Himachal Pradesh University

Abstract- *Information security and data protection have become extremely important for communication over public channels thus necessitating the use of cryptography to protect communication. Cryptography is a strategy towards assurance a safe transaction between the sender and the receiver. Moreover, only the authorized receiver can have the right to decrypt the information that was sent and encrypted by the sender in this paper, we present a detailed analysis of asymmetric key algorithms. Firstly, this paper presents the basic concepts of Cryptography which are encryption and decryption operations. Secondly, it compares the common asymmetric algorithms Rivest Shamir Adleman (RSA), El-Gamal, Elliptic Curve (ECC). Digital Signature Algorithm DSA, and Diffie Hellman. Our comparison is based on the key size, areas of implementation, and their strengths and weaknesses that affect the running time.*

Keywords- Rivest Shamir Adleman (RSA), Diffie-Hellman, Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA), El Gamal, Differences, Comparison.

I. INTRODUCTION

Cryptography is "the art of writing or solving codes". [1]. Cryptography is a Greek word that is a combination of two words cryptos which means "hidden or secret" and graph which means "to write or study." So, cryptography is well-defined as "the study of hidden secrets". Cryptography is securing information from unauthorized access or a person by transforming it into a form unrecognizable and unreadable to an unauthorized person during the transmission of data. Data can be in any form text, image, audio, video, or any other format. Cryptography is a security tool utilized to secure email messages, credit card data, corporate information, and any relevant data transmitted through all types of media and various fields like wired networks and wireless networks.
Cryptography is classified into two major categories: Symmetric Key Systems (Fig1.1) and Asymmetric Key systems (Fig 1.2).

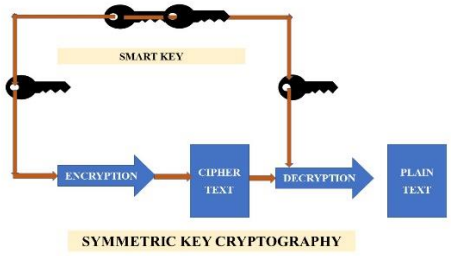

Fig. 1.1. The general idea of symmetric-key cryptography

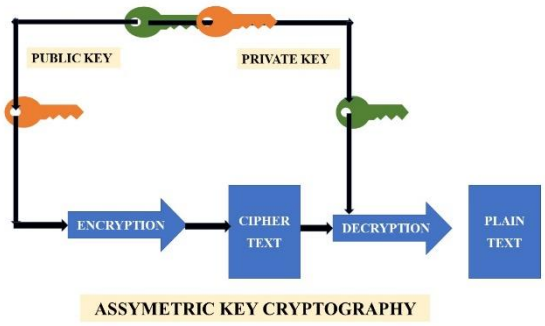

Fig. 1.2. The general idea behind asymmetric-key cryptography

A. Cryptography

Cryptography is hiding information in a systematic manner such that only authorized parties have access to the data.it is a science. Cryptosystems are broadly classified into two major categories, first is symmetric and the other is asymmetric based on the concepts of the key.

B. Terminology

This section deals with the description of some of the concepts used in cryptography:

***Plain Text*:** The master copy message is to be sent from the sender to the recipient. This plain text is kept as input at the time of encryption action. For example, if the sender wants to send a message "hello" to the receiver then it is regarded as plain text.

***Cipher Text*:** The text which is being sent from sender to receiver is not understandable by anybody and it is the output of the encryption work. For example: "*#85K&" is a cipher text produced for a plain text "hello".

***Encryption*:** The process of encoding plain text messages into cipher text messages is called encryption.

***Decryption*:** The reverse process of transforming cipher text messages back to plain text is called decryption.

Keys: A Key is a numeric or alphanumeric text or maybe a special character. The key is applied at the time of encryption carries a place on the plaint text and at the time of decryption takes a place on the cipher text. The choice of the key in cryptography is very important as the security of the encryption algorithm depends directly on it.

- *Symmetric key*: Just single key is utilized in both encrypting and decrypting processes.
- *Asymmetric key*: Asymmetric use two different keys: one for encryption and one for decryption. This system is also known as a public key Crypto system.

II. LITERATURE REVIEW

Menezesetal.[2] defines cryptography as it is a study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is not the only means of providing information security, but rather one set of techniques.

J. Zhou,etal. [3] in their paper "Research and implementation of RSA algorithm for encryption and decryption" encryption and decryption end result can make sure the privacy of the data, as well as the integrity of data. This paper contains a complete discussion of the cryptography, encryption, decryption, and RSA public key and other related technology operations in the service, business, sequestration and other fields of information security which plays an important part. In summary, this issue of the RSA encryption and decryption keys, RSA algorithm, the new use of the RSA and other issues to study and make some new programs, future work should be in the new RSA cryptographic algorithms and a wide range of operations continue to probe.

Mallouli et al. [4] This paper presents a check of the main important cryptographic algorithms ECC, El-Gamal and RSA. These algorithms are studied in order to be compared. Comparisons prove that the cost of transmission is tremendously reduced in ECC. The result shows the performance of ECC that are useful.

Kaur et al. [5] Describes that there are different types of encryption ways are being used to ensure the sequestration of data transmitted over internet. Digital Hand is a fine scheme which ensures the sequestration of discussion, integrity of data, authenticity of digital communication/ sender and non-repudiation of sender. Digital Hand is bedded in some tackle device or also exits as a train on a storehouse device. Digital Hand are inked by third party some certifying authority. This paper describes the different crucial factor of digital hand with the working of digital hand, through colorful styles and procedures involved in subscribing the data or communication by using digital hand. It introduces algorithms used in digital autographs.

Mikhai et al [6] Describes that the security is an essential demand in the artificial world. Information leakage to challengers can beget fiscal problems for a company. Also, the wide use of the Internet as an terrain for doing business and shopping calls for secure electronic deals. Confidentiality of the information is saved through the use of encryption schemes. This paper proposes a new three- party extension of El Gamal encryption scheme and multi-receiver extension of El Gamal encryption scheme. For both of the two proposed schemes, security and performance are anatomized. Eventually, the operation of El-Gamal encryption scheme in internet voting is studied for its significance currently.

Neha et al. [7] They compare asymmetric algorithms like RSA, OAEP, Elliptic curve cryptography in this paper which is used for security when data is transmitting over the network. When they compare elliptic curve cryptography with RSA then they identify that ECC provides less overhead compare to the RSA. In case of encrypting the text ECC is much better than RSA algorithm. RSA gives better security for the business application so this can be valuable for encryption of long messages without any hybrid and symmetric encryption.

Ernest [8] describes some of the different computational algorithms that have been used in the chip designs and to provide a list of all of the currently available chips.

Ghosh et al. [9] designs a hybrid algorithm by combining AES-DES-RSA and incorporating it in the Feistel structure. The proposed algorithm is compared with AES, DES, and RSA and evaluated on three parameters. They conclude that Hybrid AES-DES algorithm Key Exchange Mechanism has better avalanche effect

a) RSA

It is named after the three inventors- Ron Rivest, Adi Shamir, and Leonard Adleman. It is developed back in 1978 RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem [10]

Strengths:[11]

- terms of authenticity and confidentiality, RSA overcomes all symmetric algorithms' flaws.
- For encryption, it is quicker than DSA (Digital signature algorithm).
- Decoding the RSA algorithm is difficult as it requires complex mathematical calculations.
- Easy to implement. It is also simple to share public keys with users.

Weakness:

- With the RSA algorithm, there's just too much computation going on.
- The encryption and decryption processes take a long time, and generating keys is cumbersome.
- There is no evidence that a compromised RSA will require factorization, hence it is not logically possible to say that RSA security depends on how difficult it is to factor huge numbers[12]
- If there is an algorithm that can fast decompose a large number, so the RSA algorithm's security would be threatened. [12]

b) DIFFIE HELLMAN

This asymmetric algorithm is used for exchanging cryptography keys between two users. Diffie--Hellman developed this algorithm in 1976. Here, users employ a shared secret key through an unsecured communication channel without knowing each other's keys, and then they use this key to encrypt subsequent conversations using a symmetric key cipher. [13]

Strengths:[14]

- The sender and receiver don't need any prior knowledge of each other.
- Data transmission across an unsafe channel is possible after the keys have been exchanged.
- The sharing of the secret key is safe.

Weakness:

- the main disadvantage of this algorithm is that the communication is performed through it which means that it can be violated in the middle of the attack
- The DIFFIE- Hellman key exchange is vulnerable to a man-in-the-middle attack because it doesn't need any parties to the communication to provide authentication.
- Similarly, it cannot be used for signing digital signatures.[15]

c) ECC

Elliptic curve cryptography is apublic-key(asymmetric) algorithms that can give shorter key size based upon the environment. First described in 1985 by two independent teams and the application in which it is used, improved the performance of system-based discrete logarithms [16]

Fig c.1 shows Elliptic Curve which is a plane curve defined as the equation $Y^2=f(x)$ where f(x) is defined by a cubic polynomial with no repeated roots.[17]

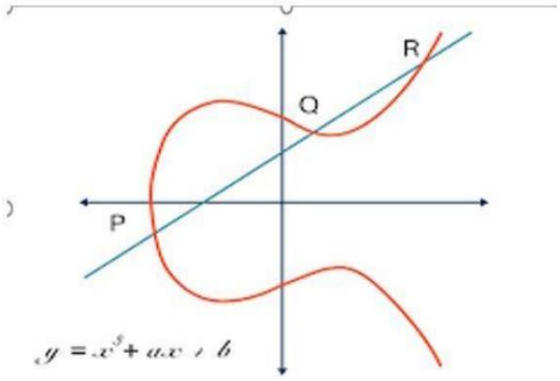

Fig c.1: Elliptic Curve [17]

Strengths: [18]

- ECC has performance advantages (fewer computations) and bandwidth advantages (shorter signatures and keys) over RSA and Discrete Logarithm (DL) schemes.
- To decode an encrypted message, the encryption method needs to be supplied with the relatively small encryption key used by ECC. Compared to other public key encryption methods from the first generation, this short key is quicker and uses less processing power.
- The advantages of ECC over RSA are particularly important in wireless devices, where computing **power, memory, and battery life are limited.**

Weaknesses:

- ECC's primary drawback is that it greatly increases the size of the encrypted message compared to RSA encryption.
- Furthermore, the ECC algorithm is extra complex plus more hard to put into practice than RSA, which increments the chances of implementation mistakes, thus reducing the security of the algorithm.

d) DIGITAL SIGNATURE ALGORITHM (DSA):

It is used by the recipient of a message to verify that the sender's identity and message has not been altered during transit. Due to the fact it may be used to demonstrate to the receiver or a third party that something is authentic, a digital signature is an electronic equivalent of a written signature. It was proposed in 1991 and globally standardized in 1994 by the National Institute of Standards and Technology (NIST). Digital signatures can be generated for stored data and programs therefore truthfulness of the data and programs can be confirmed [19].

Asymmetric key systems typically use a public key for encryption along with a private key for decryption. The opposite is true, however, for digital signatures. The public key is used to decrypt the signature once it has been encrypted using the private key. Because the keys are linked, decoding it with the public key verifies that the proper private key was used to sign the document, thereby verifying the signature's provenance

Strength:[20]

- Along with having strong strength levels, the signature's length is smaller compared to other digital signature standards.
- The signature computation speed is less.
- DSA requires less storage than other digital standards to function.
- DSA is patent-free so it can be used free of cost.

Weaknesses:

- It requires a lot of time to authenticate as the verification process includes complicated remainder operators. It requires a lot of time for computation.
- Data in DSA has not been encrypted the digital signature algorithm first computes with SHA1 hash and signs the data, which is the only way we can verify it. DSA is inherently dependent on SHA1, therefore any flaws in its cryptography security will be mirrored in it.
- DSA is a US National Standard that has uses in both secret and non-secret communications

e) EL GAMAL

The El Gamal cryptosystem is a public-key encryption scheme proposed by Taher El Gamal in 1985. The El Gamal cryptosystem essentially turns the Diffie-Hellman key exchange method into an encryption algorithm. The security of the El Gamal algorithm is based on the difficulty of solving the Diffie Hellman Problem (DHP) in $Z*$

Strengths:[21]

- The main strength of El Gamal is that it employs randomized encryption to provide enhanced cryptographic security.
- Every time a plaintext is encrypted a different ciphertext results. This is because the private key d is a randomly chosen integer which is different for each encryption (similar to the one-time pad).

Weakness:

- Firstly, the cipher text is expanded by a factor of two meaning that the cipher text size is twice as long as the plain text [22].
- Secondly, the encryption operation is unconditionally malleable or can be changed without following any condition, thus making it prone to the chosen cipher text attack.
- The third weakness of El Gamal is the possibility of forged signatures, especially if the message is not signed, thus making it vulnerable to a man-in-the-middle attack because the recipient cannot be able to detect that the message's contents were altered. However, this problem can be overcome by implementing a web of trust or through the use of a central certification authority [23].

III. COMPARATIVE ANALYSIS

The following tables describe the comparison table of different asymmetric algorithms based on key size, strength, weakness, possible attack, preferable countermeasures of attacks, and analysis [24][25].

Table 1.1: ComparisonBasedon Strengths

Parameters	RSA	Diffie Hellman	DSA	ECC	El Gamal
Made in Year&Developer [26]	1998 by Ron Rivest et.al	1976 by Hellman	1994 by NIST	1985 by Neal Koblitz and Victor Mille	1985 by ElGamal
Implementation	Easy	Relatively Hard	Medium	Hard	Medium
Power Consumption	Low	High	Medium	Medium	Medium
Time Consumption	Slowest	Medium	Medium	Fast	Medium
Key Size	Large	Medium	Medium	Smaller	Smaller

Each algorithm has its strengths based on the scenario is used.

After looking at all the encryption techniques defined above, we can conclude that ECC is faster than RSA because it uses smaller keys. However, its mathematical operations are more complex than RSA. The Diffie-Hellman encryption algorithm exchanges a secret key between two users. A digital signature is issued by the receiver on the DSA to verify that the received signal has not been altered.

Every Asymmetric algorithm has its Weaknesses that's why we use specific algorithm for specific purposes, above table describes the weaknesses of the algorithms.

Table 1.3:Comparison Based on Possible Attacks [27]

Algorithm	Possibleattacks
RSA	• Adaptivechosencipher textattack • Powerfault attack • Sidechannelanalysisattack
DIFFIE-HELLMAN	• Manin the middleattack.
DSA	• Keyrecoveryattack. • Latticeattacks.
ECC	• Side-channelattacks • Side channel attacks. • Back doors Quantum
ElGamal	BonehJouxand NguyenAttacks

Key Sizes that can be in the Asymmetric Algorithms are discussed in the above table.

Table: Comparison Based on Key Size:

Algorithm	Keysize(in bits)
RSA	1024 (can be breakable in the near future) 2048 3027 4096
DIFFIE-HELLMAN	1024or 3072 for p (the modulus)
DSA	Multipleof64; between512& 1024(inclusive)
ECC	Smaller key sizes 160 224 256
ElGamal	>1024

IV. CONCLUSION

After analysis, we can conclude that ECC provides less computation cost and less power requirement. But one of the major advantages of using ECC over other encryption techniques is that it provides more security even using smaller keys. The security provided by ECC of 112 bits key size is the same as that of security provided by RSA or DSA for a key of size 512 bits. Since RSA is vulnerable to some attacks but ECC is in its adaptive phase. ECC keys are smaller and can be computed faster as compared to RSA. E.g., a 256-bit ECC provides equivalent security to that of 3072 bits RSA. Functions in ECC have less computation cost. To keep low power and low-cost system we use ECC. ECC provides faster SSL handshaking and faster web page loading. ECC can be said to be the optimum solution when it comes to network security. After reviewing all the above-defined cryptography techniques, it can be concluded that ECC is faster than RSA because it uses small key. However, its mathematical operations are more complicated than RSA. The Diffie-Hellman encryption algorithm exchanges a secret key between two users. A digital signature is used by her DSA recipient to verify that the received signal has not been altered [28].

V. FUTURE SCOPE

This work has numerous opportunities for future investigation, report mainly concentrated on comparative analysis of asymmetric algorithms such as RSA, DSA, El Gamal, Diffie Hellman, and ECC. Future work can be focused on adding some new features to other cryptography algorithms and doing practical Implementation on them. For systems that have limited resources available and less computation power. ECC is gaining a lot of popularity. It is estimated that by the end of

2030 most of the encryption will be based on ECC leaving behind RSA. Since ECC provides us more security even with lesser keys, it requires less computation power and gives a better user experience. Block chaining in IoT devices and applications is gaining immense popularity nowadays and to provide security in IoT applications ECC will be used in blockchain technology and most IoT devices in the future. ECC along with AES is gaining huge popularity. In the future, we can compare the performance of ECC along with other encryption techniques to Ensure better security and find the best algorithm and maximize the speed and security.

REFERENCES

[1] Verma, R. and Sharma, A.K., 2020. Cryptography: Avalanche effect of AES and RSA. International Journal of Scientific and Research Publications, 10(4), pp.119-125

[2] Menezes, A.J.,1997.PCvanOorschot andSAVanstone. Handbook ofapplied cryptography, pp.490-524

[3] Zhou,X.andTang,X.,2011,August.Researchandimplement ation. ofRSAalgorithmfor encryption and decryption. In Proceedings of 2011 6th international forum on strategic technology (Vol. 2, pp. 1118-1121). IEEE.

[4] Mallouli, F., Hellal, A., Saeed, N.S. and Alzahrani, F.A., 2019, June. A survey on cryptography: comparative study between RSA vs ECC Algorithms, and RSA vs El-Gamalalgorithms.In20196thIEEEInternationalConference onCyberSecurityand Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 173-176). IEEE.

[5] Kaur,R.andKaur,A.,2012,September.Digitalsignature.In20 12International Conference on Computing Sciences (pp. 295-301). IEEE.

[6] Garg,N.andYadav,P.,2014.Comparisonofasymmetricalgor ithmsincryptography. Journal of Computer Science and Mobile Computing (IJCSMC), 3(4), pp.11901196.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[8] S. A. Ritu Tripathi, "Comparative study of symmetric and asymmetric cryptography techniques," International Journal of Advance Foundation and Research in Computer, vol. 1, 2014

[9] Gupta Shubhi, Department of Computer Science and Engineering, Amity university, Greater Noida, "Implementation of ECC using socket programming in Java", International Organization of Scientific Research (IOSR), , Volume 16, Issue 4, Ver. I (JulAug. 2014), PP 87-89

[10] Mikhail, M., Abouelseoud, Y. and Elkobrosy, G., 2014, January. Extension and applicationofEl-Gamalencryptionscheme.In2014WorldCongressonComputer Applications and Information Systems (WCCAIS) (pp. 1-6). IEEE.

[11] S. A. Ritu Tripathi, "Comparative study of symmetric and asymmetric cryptography techniques," International Journal of Advance Foundation and Research in Computer, vol. 1, 2014

[12] Jirwan, N., Singh, A. and Vijay, S., 2013. Review and analysis of cryptography techniques. *International Journal of Scientific & Engineering Research*, *4*(3), pp.1-6

[13] Aufa, F.J. and Affandi, A., 2018, August. Security system analysis in combination method: RSA encryption and digital signature algorithm. In *2018 4th International Conference on Science and Technology (ICST)* (pp. 1-5). IEEE.

[14] Yassein, M.B., Aljawarneh, S., Qawasmeh, E., Mardini, W. and Khamayseh, Y., 2017, August. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 international conference on engineering and technology (ICET)* (pp. 1-7). IEEE.

[15] Toradmalle, D., Singh, R., Shastri, H., Naik, N. and Panchidi, V., 2018, August. Prominence of ECDSA over RSA digital signature algorithm. In *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on* (pp. 253-257). IEEE

[16] Brickell, E.F., 1989, August. A survey of hardware implementations of RSA. In ConferenceontheTheoryandApplicationofCryptology(pp.368-370).Springer,New York, NY.

[17] Shubhi Gupta, DivyaSingh, SwatiVashisht&Pradeep kushwaha , "Enhancing Big Data Security using Elliptic Curve Cryptography", 2019 International Conference on Automation, Computational and Technology Management (ICACTM) Amity University.

[18] Mahto, D. and Yadav, D.K., 2017. RSA and ECC: a comparative analysis. *International journal of applied engineering research*, *12*(19), pp.9053-9061.

[19] J. Rothe, "Other public-key cryptosystems and protocols," Complexity Theory and Cryptology: An Introduction to Cryptocomplexity, pp. 361- 412, 2005

[20] J. Rothe, "Other public-key cryptosystems and protocols," Complexity Theory and Cryptology: An Introduction to Cryptocomplexity, pp. 361- 412, 2005

[21] Gaithuru, J.N., Bakhtiari, M., Salleh, M. and Muteb, A.M., 2015, December. A comprehensive literature review of asymmetric key cryptography algorithms for establishment of the existing gap. In *2015 9th Malaysian*

Software Engineering Conference (MySEC) (pp. 236-244). IEEE.

[22] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. CRC press, 1996

[23] A. Y. Meier, "The elgamal cryptosystem," 2005

[24] Singh, P., 2022. A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN. [online] research gate

[25] N. Jirwan, et al., "Review and Analysis of Cryptography Techniques", International Journal of Scientific & Engineering Research, vol. 4, iss.3, Mar2013

[26] Wei, W., Zhang, J., Wang, W., Zhao, J., Li, J., Shen, P., Yin, X., Xiao, X. and Hu, J., 2013. Analysis and Research of the RSA Algorithm. *information technology Journal*, *12*(9), p.1818

[27] Jirwan, N., Singh, A. and Vijay, S., 2013. Review and analysis of cryptography techniques. International Journal of Scientific & Engineering Research, 4(3), pp.1-6

[28] Ghosh,S.N.,2015.Performance analysisofAES, DES,RSA,andAES-DES-RSAhybrid algorithmfordatasecurity.InternationalJournalofInnovative andEmergingResearchin Engineering, 2(5), pp.83-88.

[29] Omar G. A., Elsadd, M. A., &Guirguis, S. K.: Investigation of Cryptography Algorithms used for Security and Privacy Protection in Smart Grid. In Power Systems Conference (MEPCON), 2017 Nineteenth International Middle East, IEEE, 644-649, (December 2017).

[30] Saho, N.J.G. and Ezin, E.C., 2020. Survey on Asymmetric Cryptographic Algorithms in Embedded Systems. *IJISRT*, *5*, pp.544-554.